대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출원번호 : 10-2002-0001916
Application Number PATENT-2002-0001916

출원년월일 : 2002년 01월 12일
Date of Application JAN 12, 2002

출원인 : 주식회사 코어트러스트
Applicant(s) Coretrust, Inc.

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

2003 년 01 월 10 일

특허청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2002.01.12
【발명의 명칭】	디지털 컨텐츠의 정보보호 방법 및 시스템
【발명의 영문명칭】	Method and system of the information protection for digital contents
【출원인】	
【명칭】	주식회사 에쎄소프트
【출원인코드】	1-2000-057231-4
【발명자】	
【성명】	우제학
【출원인코드】	4-2001-052513-7
【발명자】	
【성명】	이환철
【출원인코드】	4-1998-602710-3
【발명자】	
【성명】	조상영
【출원인코드】	4-2001-052512-1
【발명자】	
【성명의 국문표기】	정성호
【성명의 영문표기】	JEONG,Seong-Ho
【주민등록번호】	780703-1055811
【우편번호】	139-243
【주소】	서울특별시 노원구 공릉3동 371-9호 현대빌라 206호
【국적】	KR
【발명자】	
【성명의 국문표기】	신석균
【성명의 영문표기】	SHIN,Seog Kyoon
【주민등록번호】	720106-1031324
【우편번호】	140-132
【주소】	서울특별시 용산구 청파동2가 33-2 은행연립 가동 102호
【국적】	KR

【발명자】

【성명의 국문표기】 하영수

【성명의 영문표기】 HA,Young-Soo

【주민등록번호】 750701-1399024

【우편번호】 139-800

【주소】 서울특별시 노원구 공릉2동 240-168

【국적】 KR

【발명자】

【성명의 국문표기】 김성일

【성명의 영문표기】 KIM,Seong-il

【주민등록번호】 790304-1012314

【우편번호】 139-243

【주소】 서울특별시 노원구 공릉3동 삼익아파트 404-308

【국적】 KR

【심사청구】 청구

【조기공개】 신청

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 출원인 주식회사 에쎄소프트 (인)

【수수료】

【기본출원료】	20 면	29,000 원
【가산출원료】	34 면	34,000 원
【우선권주장료】	0 건	0 원
【심사청구료】	15 항	589,000 원
【합계】	652,000 원	
【감면사유】	소기업 (70%감면)	
【감면후 수수료】	195,600 원	

【첨부서류】 1. 요약서·명세서(도면)_1통 2.소기업임을 증명하는 서류_1통[사업자등록증, 원천징수신고서, 건 물임대차계약서]

【요약서】

【요약】

본 발명은 온라인 또는 오프라인으로 제공되는 암호화된 텍스트, 음악, 동영상강의, 영화, 소프트웨어, 게임 등 모든 형태의 디지털 컨텐츠의 불법복제 및 불법전송 등의 저작권 침해행위를 원천적으로 차단하는 정보보호 방법 및 시스템에 관한 것이다.

본 발명의 목적은 암호화된 컨텐츠를 보기위한 전용뷰어프로그램를 대신에 일반 응용프로그램을 사용할 수 있고, 다운로드 도중에 스트리밍으로 컨텐츠를 볼 수 있는 한층 보안성능을 높이는 방법 및 시스템과 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는 것이다.

본 발명의 특징은 사용자 컴퓨터의 디바이스 드라이버 단계에서 파일입출력요청 메시지를 후킹하여 메시지의 발생, 변형, 또는 삭제를 함으로서 일반 응용프로그램을 이용할 수 있는 방법을 제시하는 것이다. 구체적으로는 DRM 디바이스 드라이버 단계에서 응용프로그램이 요청하는 파일옵셋과 파일길이의 메시지를 변형하고, 버퍼메모리상에서 복호화하고, 원래 응용프로그램이 요청한 파일옵셋 및 파일길이 형태의 복호화된 데이터를 복원하여 응용프로그램에 전달하는 방법을 제공하는 것이다.

따라서 본 발명은 디지털 컨텐츠를 복호화된 상태로 어떤 저장장치에 보관하지 않고, 버퍼메모리 상에서만 일정단위로 쪼개진 데이터를 연속적으로 복호화하여 응용프로그램에 전달하기 때문에 암호화가 깨질 염려가 거의 없는 정보보호 방법을 제공하고 있으며, 온라인으로 연결된 DRM 인증서버에서 사용자 인증과 응용프로그램의 등록 및 인증, 관리

를 수행함으로서 사용의 편리성과 업그레이드 관리의 용이성을 크게 향상시키는 효과를 제공한다.

【대표도】

도 5

【색인어】

디지털 컨텐츠, 정보보호, 디지털저작권관리, Digital Rights Management, DRM, 디바이스 드라이버

【명세서】

【발명의 명칭】

디지털 컨텐츠의 정보보호 방법 및 시스템 {Method and system of the information protection for digital contents}

【도면의 간단한 설명】

도 1은 기존의 DRM 프로그램에 적용한 필터단 시스템을 나타내는 모식도.

도 2는 본 발명의 디지털 컨텐츠의 정보보호 시스템을 나타내는 모식도.

도 3은 본 발명의 DRM 제어기와 인증서버간의 응용프로그램 인증 및 사용자 인증 방법의 모식도.

도 4는 DRM 인증서버의 응용프로그램 등록 및 관리 현황을 보여주는 화면의 예시도.

도 5는 본 발명의 DRM 시스템의 구성 및 작동을 나타내는 모식도.

도 6은 암호화된 디지털 컨텐츠의 열기 과정을 보여주는 흐름도.

도 7은 암호화된 디지털 컨텐츠의 읽기 과정을 보여주는 흐름도.

도 8은 암호화된 디지털 컨텐츠의 닫기 과정을 보여주는 흐름도.

도 9는 응용프로그램 종료 과정을 보여주는 모식도.

도 10은 암호화된 디지털 컨텐츠의 복호화 과정을 보여주는 모식도.

도 11은 암호화된 디지털 컨텐츠의 파일옵셋 및 파일길이를 처리하는 과정을 보여주는 모식도.

도 12는 암호화된 컨텐츠 패키지 파일의 데이터 구조를 보여주는 모식도.

도 13은 라이센스 파일의 데이터 구조를 보여주는 모식도.

도 14는 본 발명의 일실시예에 따른 DRM이 적용된 HTTP 스트리밍을 보여주는 동영상강의 화면의 예시도.

<도면의 주요부분에 대한 설명>

200: DRM 클라이언트 프로그램 210: DRM 제어기

220: DRM 디바이스 드라이버 230: DRM 인증서버

240: 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<19> 본 발명의 목적은 온라인 또는 오프라인으로 제공되는 디지털 컨텐츠의 정보보호 방법 및 시스템에 관한 것으로서, 좀 더 상세하게는 암호화된 텍스트, 음악, 동영상강의, 영화, 소프트웨어, 게임 등 모든 형태의 디지털 컨텐츠의 불법복제 및 불법전송 등의 저작권 침해행위를 원천적으로 차단하고, 전용뷰어프로그램를 사용하지 않고 일반 응용프로그램을 사용해서 컨텐츠를 볼 수 있고, 다운로드 중에 스

트리밍으로 컨텐츠를 볼 수 있으며, 또한 디바이스 드라이버 단계에서 파일입출력요청 메시지를 후킹(hooking)하여 응용프로그램을 제어함으로서 한층 보안성능을 높인 디지털 컨텐츠의 정보보호 방법 및 시스템과 프로그램 기록매체를 제공하는 것이다.

<20> 최근 컴퓨터와 인터넷, 저장매체 등의 급속한 발전에 따라 각종 문서와 컨텐츠 등이 컴퓨터가 읽을 수 있는 디지털 데이터 형태로 제작되어 유통되고 있으나, 이러한 디지털 컨텐츠의 특성상 원본과 동일한 복사본 또는 변형본을 쉽게 만들어 낼 수 있을 뿐만 아니라 손쉽게 배포할 수 있게 되었다. 따라서 많은 자금과 시간, 창의력, 노동력이 들어가는 디지털 컨텐츠의 저작자 입장에서는 자신의 저작권을 온라인 또는 오프라인에서 철저한 보호를 원하지만, 상술한 바와 같은 디지털 컨텐츠의 손쉬운 복제성 및 배포성 때문에 디지털 컨텐츠 시장의 활성화에 큰 장애가 되고 있다.

<21> 이러한 디지털 컨텐츠의 불법복제 및 불법배포 문제를 해결하고자 나온 방법 중의 하나가 스트리밍(streaming) 방법이다. 스트리밍 방법은 사용자의 하드디스크에 데이터를 저장하는 것이 아니라 램메모리 상에서만 일시적으로 저장 및 사용이 가능하도록 한 것이지만, 이것은 통신속도 또는 기타 압축 등의 기술적인 문제로 동영상의 끊김, 버퍼링, 엉김 등이 자주 발생하는 단점이 있다. 또한 2001년 7월에 (주)훈넷에서 개발한 하이넷 레코더(Hi Net Recorder)라는 프로그램은 상기 스트리밍 방식으로 서비스되는 인터넷상의 영화, 인터넷방송, 음악, 동영상강의, 뮤직비디오 등을 스트리밍과 동시에 다운로드하여 할 수 있음을 보여줌으로서, 스트리밍 방식으로 제공되는 디지털 컨텐츠의 서비스가 불법복제에 취약함을 확인하는 계기가 되었다.

<22> 따라서 디지털 컨텐츠의 저작권을 보호하기 위해서 최근 관심이 고조되고 있는 것이 디지털저작권관리(DRM, Digital Rights Management) 시스템이다. DRM 시스템이란 다양한 채널을 통해 유통되는 텍스트, 음악, 이미지, 영상, 동영상강의, 영화, 소프트웨어, 게임 등 각종 디지털 컨텐츠를 불법 복제로부터 보호하고 지속적인 컨텐츠 유료화 서비스를 가능하게 하는 기술이다. 최근 음악파일 무료 다운로드 사이트인 미국의 냅스터에 대한 서비스 중지 판결과 한국판 냅스터인 소리바다에 대한 저작권협회의 소송으로 DRM 시스템에 대한 관심은 어느 때 보다 높아진 상황이며, 이와 같은 저작권 침해 논란을 해결해 줄 수 있는 유일한 대안으로 많은 연구개발 및 상품화가 진행되고 있다. 따라서 컨텐츠 공급자가 DRM 시스템를 도입하면 모든 네트워크를 통해 유통되는 디지털 컨텐츠는 컨텐츠 공급자가 정한 규칙과 사용정책을 충족할 경우에만 열어볼 수 있으며, 불법복제를 하더라도 모든 디지털 컨텐츠는 암호화되어 있어 정당한 비용을 지불하지 않은 사용자는 열어 볼 수가 없게 된다.

<23> 현재 DRM 관련업체는 크게 DRM 원천기술 제공업체와 DRM 상용화 서비스 개발업체 등 두 가지로 나뉜다. 고도의 암호화 기술을 요하는 DRM 원천기술은 세계적으로 미국의 인터트러스트(www.intertrust.com), 마이크로소프트(Microsoft), IBM, 컨텐츠가드(www.cotentsguard.com) 등 3, 4개 업체만이 보유하고 있다. 인터트러스트는 직접 DRM 상용화에 나서고 있지는 않으며 라이선스 계약을 통해 각국 주요 IT업체들에게 원천기술을 제공하고 있다. 마이크로소프트는 최근 음악, 동영상 등 디지털 컨텐츠에 대한 저작권 보호를 위한 윈도우미디어저작권매니저(WMRM, Windows Media Rights Manager)이라는

툴을 자체적으로 선보였다. 또한 독자적으로 DRM 기술을 개발하고 있는 국내 업체들도 최근 속속 등장하고 있으며, 대표적인 업체들이 파수닷컴(www.fasoo.com), 마크애니(www.markany.com), 엔피아(www.enpia.com), 디지캡(www.digicaps.com), 테르텐(www.teruten.com), 아르파(www.arpasec.com), 실트로닉(www.sealtronic.com), 드림인테크(www.dreamintech.com) 등이 있으며 치열한 기술개발 경쟁을 벌이고 있다.

<24> DRM 시스템과 관련하여 현재까지 개발된 기술들은 주로 다운로드에 의해 사용자 컴퓨터에 저장되어 있는 암호화된 디지털 컨텐츠에만 적용되거나, 컨텐츠를 보기 위한 전용뷰어프로그램에 DRM 제어기를 내장시킨 방식이 대부분이다. 다운로드 방식에만 적용되는 DRM 시스템의 경우 인터넷영화나 동영상 강의와 같은 대용량의 컨텐츠에 적용하기에는 다운로드 시간이 너무 많고, 하드디스크의 용량에 부담이 생기고, 스트리밍을 지원하지 못한다는 단점이 있다. 컨텐츠를 보기 위한 전용뷰어 프로그램에 DRM 제어기가 내장된 경우, 지원되는 컨텐츠 데이터의 파일형식에 제한이 생기고, 수많은 파일형식과 응용프로그램에 대응하는 각각의 전용뷰어프로그램들을 제작해야 하며, 또한 지속적인 전용뷰어프로그램의 업그레이드가 필요한 단점이 있다.

<25> 최근 전용뷰어프로그램의 단점을 해소하는 기술로 제안된 것은 '디지털 데이터의 안전한 전달 및 실행을 위한 보안 시스템(한국특허출원 10-2001-00383, 주식회사 테르텐)'이다. 도 1은 상기 특허출원의 대표도면으로서 일반적인 DRM 프로그램에 적용한 필터단 시스템을 나타내는 모식도이다. 상기 특허의 핵심기술은 클라이언트 시스템의 저장장치에 특정저장영역A(120)를 별도로 생성하고, 특정 실행 프로그램만이 상기 특정저장영역A에

접근할 수 있도록 필터단을 제어하는 필터단 제어기와, 상기 특정영역내의 모든 데이터의 입출력을 제어하면서 등록된 실행프로그램(B.exe)의 데이터 호출만을 유효한 것으로 판정하여 실행하도록 하는 파일시스템 필터단(130)으로 구성되어 있다. 그러나 상기 기술은 필터단을 통해 응용프로그램을 제어하는 일반적인 기술을 포괄적으로 기술한 것이며, 저장장치 내에 별도관리를 하는 특정저장영역A를 부가적으로 설치가 필요하며, 특정저장영역A에는 복호화된 데이터를 보관함으로서 보안상의 허점이 발생할 수 있으며, 응용프로그램의 등록을 파일시스템 필터단에 모두 등록 및 관리하여야 하며, 암호화 및 복호화에 대한 구체적인 기술적인 언급이 거의 되어있지 않다.

【발명이 이루고자 하는 기술적 과제】

<26> 본 발명의 목적은 디지털 컨텐츠의 불법복제 및 불법전송 등의 문제점을 해결할 수 있는 디지털 컨텐츠의 정보보호 방법 및 시스템, 프로그램 기록매체를 제공하는 것이다.

<27> 본 발명의 또 다른 목적은 별도의 저장장치 내에 별도의 특정저장영역을 사용하지 않고, 복호화된 상태로 어떤 저장장치에 보관하지 않고, 버퍼메모리 상에서만 일정단위로 쪼개진 데이터를 연속적으로 복호화하여 응용프로그램에 전달하기 때문에 암호화가 깨질 염려가 거의 없는 정보보호 방법을 제안하는 것이다.

<28> 본 발명의 또 다른 목적은 온라인으로 연결된 DRM 인증서버에서 사용자 인증과 응용프로그램의 등록 및 인증, 관리를 수행함으로서 사용의 편리성과 업그레이드 관리의 용이성을 크게 향상시키는 것이다.

<29> 본 발명의 또 다른 목적은 디바이스 드라이버 단계에서 파일입출력요청 메시지를 후킹하여 메시지의 발생, 변형, 또는 삭제를 함으로서 응용프로그램을 제어하기 때문에, 암호화된 컨텐츠를 보기위한 전용뷰어프로그램 대신에 일반 응용프로그램을 이용할 수 있는 방법을 제안하는 것이다.

<30> 본 발명의 또 다른 목적은 DRM 디바이스 드라이버 단계에서 응용프로그램이 요청하는 파일옵셋과 파일길이의 메시지를 변형하고, 복호화하고, 원래 응용프로그램이 요청한 파일옵셋 및 파일길이 형태의 복호화된 데이터를 응용프로그램에 전달하는 방법을 제공하는 것이다.

<31> 본 발명의 또 다른 목적은 암호화된 디지털 컨텐츠의 정보보호를 다운로드된 것 뿐만 아니라, 다운로드 과정의 수행과 동시에 HTTP 스트리밍 방식을 지원하는 기술을 제공하는 것이다.

【발명의 구성 및 작용】

<32> 상기와 같은 목적을 달성하기 위한 본 발명의 디지털 컨텐츠의 정보보호 시스템은, 온라인 또는 오프라인으로 컨텐츠 배포자(260)로부터 제공받아 사용자 컴퓨터에 저장된 암호화된 컨텐츠 패키지(240)를 선택하여 열면 자동으로 DRM 제어기(210)가 구동하여 컨텐츠 패키지 헤더(1010) 속에 포함된 파일이름 및 파일크기, 서버정보, 컨텐츠 정보 등을 수집하여 분석하는 정보분석수단과, 상기 패키지 헤더의 정보분석을 바탕으로 DRM 제어기가 인터넷으로 연결된 DRM 인증서버(230)로 부터 응용프로그램 인증 및 사용자 인증을

수행하는 인증수단과, 상기 인증결과를 바탕으로 DRM 제어기가 획득한 라이센스 파일을 이용하여 컨텐츠의 사용기간 또는 사용횟수, 사용가능한 컴퓨터의 숫자 등의 관리를 하는 라이센스 관리수단과, 상기 암호화된 컨텐츠 패키지를 볼 수 있는 응용프로그램의 기동 및 제어, 종료 등을 수행하는 제어수단과, DRM 디바이스 드라이버(220)가 응용프로그램과 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템간의 열기, 읽기, 닫기, 종료 등의 파일입출력요청 메시지를 가로채는 디바이스 드라이버 단계의 후킹 수단과, 상기 디바이스 드라이버 단계의 후킹 정보인 응용프로그램이 파일시스템에 요청한 파일옵셋 및 파일길이의 정보변형수단과, 상기 변형된 파일옵셋 및 파일길이의 정보를 바탕으로 암호화된 컨텐츠 패키지의 데이터를 버퍼메모리로 가져와서 복호화하는 복호화 수단과, 상기 버퍼메모리에서 복호화된 컨텐츠 패키지의 데이터를 응용프로그램이 요청했던 파일옵셋 및 파일길이 형태로 복원하는 복원수단과, 상기 복호화되어 복원된 컨텐츠 패키지의 데이터를 응용프로그램에 전달하는 전달수단을 포함하는 것을 특징으로 한다.

<33> 또한, 상기 목적을 달성하기 위한 본 발명의 디지털 컨텐츠의 정보보호 방법은, 온라인 또는 오프라인으로 컨텐츠 배포자(260)로부터 제공받아 사용자 컴퓨터에 저장된 암호화된 컨텐츠 패키지(240)를 사용자가 선택하여 열면 자동으로 DRM 제어기(210)가 구동하는 단계(S51); 상기 DRM 제어기가 컨텐츠 패키지의 헤더(1010) 속에 포함된 파일이름 및 파일크기, 서버정보, 컨텐츠 정보 등을 수집하여 분석하는 단계(S52); 상기 패키지 헤더의 정보분석을 바탕으로 DRM 제어기가 인터넷으로 연결된 DRM 인증서버(230)로부터 응용프로그램 인증 및 사용자 인증을 수행하여 라이센스 파일의 정보를 획득하는 단계(S53); DRM 제어기가 응용프로그램에게 프로세스 식별자를 생성한 후 응용프로그램의 실행을 잠

시 중지하는 단계(S54); DRM 제어기가 DRM 인증서버로부터 획득한 라이센스 및 응용프로그램 인증정보를 DRM 디바이스 드라이버에 등록시키는 단계(S55); 상기 잠시 중지된 응용프로그램이 다시 구동하여 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템에 파일옵셋과 파일길이를 요청하는 파일입출력요청 메시지를 DRM 디바이스 드라이버에서 후킹하는 단계(S56); 상기 후킹된 파일입출력요청 메시지의 파일옵셋과 파일길이를 암호화된 컨텐츠 패키지의 형태에 맞추어 변형해주는 단계(S57); 상기 변형된 파일옵셋과 파일길이에 맞게끔 암호화된 컨텐츠 패키지의 데이터를 임시저장공간인 버퍼메모리에 로딩하여 복호화하고 원래 응용프로그램이 요청한 파일옵셋과 파일길이에 맞게끔 복호화된 컨텐츠 패키지의 데이터를 복원하는 단계(S60); 및 상기 복원된 파일옵셋과 파일길이에 맞게끔 복호화된 컨텐츠 패키지의 데이터를 응용프로그램에 전송하는 단계(S61)를 포함하는 것을 특징으로 한다.

<34> 또한, 상기 목적을 달성하기 위한 본 발명의 기록매체는, 디지털 컨텐츠의 정보보호 시스템에, 온라인 또는 오프라인으로 컨텐츠 배포자로부터 제공받아 사용자 컴퓨터에 저장된 암호화된 컨텐츠 패키지를 사용자가 선택하여 열면 자동으로 DRM 클라이언트 프로그램(200)이 구동하여 컨텐츠 패키지의 헤더 정보를 분석하는 기능; 상기 정보분석을 바탕으로 DRM 클라이언트 프로그램이 인터넷으로 연결된 DRM 인증서버로 부터 응용프로그램 및 사용자 인증을 수행하는 기능; 상기 인증결과를 바탕으로 라이센스를 획득하여 라이센스를 관리하는 기능; 상기 DRM 클라이언트 프로그램이 상기 컨텐츠 패키지를 볼 수 있는 응용프로그램의 기동 및 제어, 종료 등을 제어하는 기능; 상기 응용프로그램과 파일시스템간의 파일입출력요청 메시지를 디바이스 드라이버 단계에서 가로채는 후킹기능;

상기 후킹 정보의 파일옵셋 및 파일길이를 변형하는 정보변형 기능; 상기 변형된 파일옵셋 및 파일길이를 바탕으로 암호화된 컨텐츠 패키지의 데이터를 버퍼메모리로 가져와서 복호화하는 기능; 상기 버퍼메모리에서 복호화된 컨텐츠 패키지의 데이터를 응용프로그램이 요청했던 파일옵셋 및 파일길이 형태로 복원하는 기능; 및 상기 복호화되어 복원된 컨텐츠 패키지의 데이터를 응용프로그램에 전달하는 전달기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

<35> 또한, 본 발명은 상기 응용프로그램 인증 및 사용자 인증이 DRM 인증서버에 의해 온라인으로 이루어지는 것 대신에, CD 또는 디스켓, 기타 저장장치를 통해 제공된 라이센스 파일을 이용해 오프라인으로 이루어질 수도 있다. 또한 상기 사용자 인증은 DRM 인증서버와 연동된 컨텐츠 배포자의 웹서버 또는 FTP 서버 등에서 수행한 사용자 로그인 정보를 이용하여 자동으로 DRM 인증서버에서 수행되는 인증수단 또는 단계를 더 포함할 수도 있다. 또한 상기 암호화된 컨텐츠 패키지는 하나의 암호화키 또는 여러개의 암호화키를 이용하여 암호화 및 복호화를 수행할 수도 있다. 또한, 인터넷으로 연결된 DRM 인증서버로부터 사용자 인증을 수행할 때 사용자의 패스워드 정보노출을 막아주는 양방향세션인증 단계를 더 포함할 수도 있다. 또한, 상기 DRM 디바이스 드라이버가 운영체제에서 필요한 각종 디바이스 드라이버 중 최상위 레이어에 로딩될 수 있도록, 다른 디바이스 드라이버가 로딩되는 것을 감지하면 DRM 디바이스 드라이버의 동작을 멈추게 하는 디바이스 드라이버 감시수단 또는 단계를 더 포함할 수도 있다. 또한, 상기 암호화된 컨텐츠 패키지는 사용자 컴퓨터에 저장된 것 대신에 컨텐츠 배포자로부터 사용자 컴퓨터로 다운로드 받아 저장하는 것과 동시에 HTTP 스트리밍으로 컨텐츠를 볼 수 있는 수단 또는 단

계를 더 포함할 수 있다. 또한 상기 응용프로그램이 읽어들인 복호화된 디지털 컨텐츠의 데이터를 수정 또는 편집하여 다시 저장할 수 있도록 DRM 디바이스 드라이버에 암호화 수단 또는 단계를 더 포함할 수도 있다.

<36> 상술한 목적, 특징 및 장점들은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 구체화될 것이다. 이하에서 첨부된 도면을 참조하여 본 발명의 바람직한 일실시예에 대해 상세히 설명한다.

<37> 도 2는 본 발명의 디지털 컨텐츠의 정보보호 시스템을 나타내는 모식도이다. 먼저 사용자가 인터넷 웹브라우저(280)을 통해 컨텐츠 배포자(260)의 홈페이지에서 사용자 인증(로그인)을 한 후, DRM 제어기(210)와 DRM 디바이스 드라이버(220)로 구성된 DRM 클라이언트 프로그램(200)을 엑티브엑스컨트롤(Active X control)을 이용해 자동으로 다운로드 받아서 신규 또는 업그레이드 설치(S25)한다. 사용자인증이 끝나면 사용자가 선택한 디지털 컨텐츠를 컨텐츠 배포자(260)의 웹서버 혹은 FTP 서버로부터 사용자의 컴퓨터로 다운로드(S26)를 받아서 암호화된 디지털 컨텐츠 패키지를 파일시스템(240)에 저장하게 된다. 여기서 파일시스템이란 파일에 이름을 붙이고, 저장이나 검색을 위해 논리적으로 그것들이 어디에 위치시켜야 하는지 등을 나타내는 것이며, 이와 관련한 운영체제를 일부 포함하는 개념이다. FTP 서버를 이용할 때에는 다운로드만 가능하지만, 웹서버에서 다운로드를 할 때는 HTTP 프로토콜을 이용하여 다운로드와 동시에 다운로드된 컨텐츠 패키지의 용량 안에서 HTTP 스트리밍도 가능하게 된다.

<38> DRM 제어기(210)는 사용자 컴퓨터에 저장되어 있는 암호화된 컨텐츠를 사용하려고 할 때 인터넷으로 연결된 DRM 인증서버(230)로 부터 사용자 인증 및 응용프로그램 인증을 수행하며 이에 대한 내용은 도 3에서 자세히 설명할 것이다. 상술한 바와 같이 컨텐츠 배포자의 홈페이지에 접속해서 컨텐츠를 이용하려고 할 때에는 사용자 로그인 정보를 암호화하여 온라인으로 DRM 인증서버로부터 사용자 인증을 거침으로서 사용자가 중복해서 인증을 받지 않도록 구현한다. DRM 제어기(210)는 컨텐츠 패키지 헤더의 분석 및 라이센스 관리, 응용프로그램의 기동, 제어, 종료 등의 제어기능, 그리고 DRM 디바이스 드라이버(220)의 제어를 수행한다. 컨텐츠의 라이센스 관리는 사용기간 또는 사용횟수, 사용가능한 컴퓨터 숫자 등 컨텐츠 배포자의 필요에 따라 여러 가지로 다양한 조합을 만들 수 있음은 당업자라면 손쉽게 생각할 수 있을 것이다. DRM 디바이스 드라이버(220)는 응용프로그램(250)과 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템(240) 사이에 위치하면서 파일의 열기(open), 읽기(read), 닫기(close) 등을 수행할 때의 파일입출력요청 메시지(File IOREQ, File Input/Output Request Message)를 후킹하여, 상기 메시지와 관련된 새로운 메시지의 발생, 변형 또는 삭제를 수행함으로서 일반 응용프로그램을 이용하여 암호화된 컨텐츠를 볼 수 있도록 제어하며 이에 관해서는 도 6 내지 도 8 부분에서 자세히 설명할 것이다. 또한 DRM 디바이스 드라이버는 응용프로그램이 파일의 읽기를 수행할 때 파일시스템에 요청하는 파일옵셋(file offset) 및 파일길이(file length)에 관련된 파일입출력요청 메시지를 후킹하여 변형하고, 변형된 메시지에 의해 버퍼메모리에 로딩된 암호화된 컨텐츠 패키지의 데이터를 라이센스 파일에 포함된 암호화키를 이용해 복호화하고, 상기 복호화된 데이터를 다시 원래 응용프로그램이 요청했던 파일옵셋과 파일길이 형태의 복원처리하여 응용프로그램에 전달하는 기능을 수행한다. 상기의 파일

입출력요청 메시지의 변형 및 복호화, 복원된 데이터의 전달 등 일련의 과정은 실시간으로 데이터의 완전 복호화가 끝날 때까지 연속적으로 진행된다. 또한 DRM 디바이스 드라이버는 응용 프로그램의 종료(Process kill) 메시지를 탐지하고 있다가 상기 메시지를 탐지하면 DRM 제어기에 통보하고 후킹 동작을 멈추게 되며 이에 관해서는 도 9에서 자세히 설명할 것이다. DRM 인증서버(230)는 사용자 인증 및 응용프로그램 인증을 수행하고, 인증에 성공하면 암호화키를 포함한 라이센스 파일을 사용자 컴퓨터의 DRM 제어기에 전달하는 기능을 수행한다. 상기 DRM 인증서버에서의 인증과정은 사용자 컴퓨터와 연계하여 직접 수행하거나, 상술한 바와 같이 인증서버와 인터넷으로 연결된 컨텐츠 배포자(260)와 연계하여 사용자 로그인 정보를 이용하여 자동으로 수행할 수도 있다.

<39> 도 3은 본 발명의 DRM 제어기(210)와 DRM 인증서버(230)간의 응용프로그램 인증 및 사용자 인증 방법의 모식도이다. 상술한 바와 같이 DRM 인증서버에서 응용프로그램의 인증을 수행하면 컨텐츠 배포자가 각종 디지털 컨텐츠의 암호화 및 응용프로그램의 업그레이드와 관리적 측면에서 매우 유용한 장점을 가지게 된다. 또한 양방향 세션인증을 이용하여 사용자인증을 수행하면 인터넷상에 패스워드의 이동이 없으므로 보안성능이 높아진다. 먼저 DRM 인증서버(230)의 관리자가 디지털 컨텐츠를 볼 수 있는 응용프로그램의 인증키와 파일용량을 등록시켜 놓는다. 도 4

는 DRM 인증서버의 응용프로그램 등록 및 관리 현황을 보여주는 화면의 예시도이다. 그림에서 보듯이 window media player, http 스트리밍 뷰어, GVA, Acrobat reader 등의 디지털 컨텐츠를 볼 수 있는 일반 응용프로그램을 등록시켜 놓을 수 있다. 따라서 본 발명을 이용하면 일반 문서(아래아 한글, MS워드, 훈민정음 등) 및 MS 오피스(파워포인트, 엑셀, 엑세스 등), 윈도우 미디어 플레이어, 이미지 뷰어, 동영상 강의, 음악 등의 모든 파일 형식을 지원할 수 있으며, DRM 인증서버에 손쉽게 등록하여 업그레이드 등의 관리를 수행할 수 있다. 이때 대부분의 상기 응용프로그램은 손쉽게 등록할 수 있으나, GVA 같은 동영상 강의를 수행하는 프로그램은 파일크기를 체크하는 기능이 있어 원래 파일과 암호화된 파일의 크기가 패키지의 헤더만큼 차이가 생기므로 DRM 클라이언트 프로그램을 만들 때 고려해 주어야만 한다. 도 4의 인증서버의 관리자가 화면 하단의 'Viewer 등록' 아이콘을 선택하면 응용프로그램들을 자유롭게 등록시킬 수 있으며, 화면에는 번호, 인증된 프로그램, 인증키, 설명, 파일용량, 기능 등의 정보가 표시된다. 본 발명에서 응용프로그램의 인증키는 응용프로그램의 시작점에서 128바이트 후의 16바이트 정보를 16진수로 변환하여 생성하였으며, 응용프로그램의 파일용량을 크기를 정확히 체크하여 응용프로그램의 인증정보로 사용하였으나 당업자라면 얼마든지 비슷한 유형으로 변형할 수 있을 것이다. 도 3의 사용자 컴퓨터에서 응용프로그램의 인증을 받기 위해서는 DRM 제어기(210)가 DRM 인증서버(230)에서의 인증키 생성방법과 동일한 방법으로 자동으로 응용프로그램의 인증키의 생성 및 파일용량의 체크를 수행하여 DRM 인증서버에 전송(S31)한다. DRM 인증서버는 자신이 보관하고 있는 응용프로그램의 인

증키 및 파일용량의 값과 사용자 컴퓨터에서 보내온 것을 각각 비교하여 인증성공 또는 인증실패 메시지를 사용자 컴퓨터로 전송(S32)함으로서 응용프로그램의 인증을 수행하게 된다. 만약 사용자 컴퓨터에 관련 응용프로그램이 없다면 인증실패에 관한 메시지를 띄우고, 인증에 성공하면 다음단계로 사용자 인증을 수행하며 상기의 인증순서는 큰 영향을 주지 않는다는 것은 자명하다.

<40> 도 3의 사용자 인증을 위해서는 인터넷상으로 사용자의 아이디와 패스워드가 동시에 전송되는 것을 방지하기 위해 양방향 세션인증을 채택하였다. 양방향 세션인증을 위해서는 사용자가 아이디와 패스워드를 입력하게 되면 DRM 제어기(210)에서 임의의 숫자 Rn1 (Random number 1)를 생성하여 사용자 컴퓨터의 하드웨어 정보와 컨텐츠 요청메시지, 임의의 숫자 Rn1을 사용자의 패스워드를 이용해 암호화하게 된다. DRM 제어기(210)는 상기 암호화된 것과 사용자 아이디와 사이트 정보를 DRM 인증서버(230)로 전송(S33)한다. DRM 인증서버는 사용자 아이디와 사이트 정보를 비교한 후, 임의의 숫자 Rn2를 생성하여 서버정보와 Rn1, Rn2, 요청메시지에 대한 응답메시지 등을 사용자 패스워드를 이용해 암호화하여 DRM 제어기로 전송(S34)하게 된다. DRM 제어기는 전송받은 메시지를 복호화하여 상기 생성한 Rn1과 DRM 인증서버에서 수신한 Rn1이 동일한지를 확인한 후, Rn2와 하드웨어정보, 요청메시지를 사용자의 패스워드를 이용해 암호화하고 이것과 사용자 아이디, 사이트 아이디 및 서비스 아이템 아이디 등의 정보를 DRM 인증서버로 전송(S35)한다. DRM 인증서버는 상기 수신한 정보를 복호화한 후 Rn2가 동일한 지를 비교하고 동일하면 사용자의 하드웨어 정보를 인증서버에 등록하고, 사이트 아이디와 서비스아이템 아이디의 라

이센스를 검사하고 난 후 라이센스 파일을 하드웨어 정보로 암호화하고 상기 Rn1와 Rn2를 적당히 조합하여 다시 암호화하여 DRM 제어기로 전송(S36)하게 된다. 상기 과정 중에 에러가 발생하지 않는다면 사용자는 라이센스 파일를 획득하게 되며, 상기 과정 중에 한 과정이라도 에러가 발생하게 되면 사용자 인증에 실패함으로서 이와 관련된 메시지를 사용자에게 알려주게 된다. 상술한 방법은 사용자 컴퓨터가 온라인을 이용하여 인증하는 방법이며, 또 다른 인증방법으로는 오프라인으로 CD 또는 디스켓, 기타 저장장치를 이용해 라이센스 파일(300)을 제공(S37)함으로서 인증을 수행할 수 있음은 자명한 사실이다. 따라서 본 발명의 가장 큰 장점중의 하나는 DRM이 적용된 암호화된 컨텐츠 패키지를 보기 위한 전용 프로그램을 제작할 필요가 없으며, DRM 인증서버에 등록만 시켜준다면 일반 모든 응용프로그램에 본 발명인 디지털 컨텐츠의 정보보호 시스템을 적용할 수 있다는 것이다.

<41> 도 5는 본 발명의 DRM 시스템의 구성 및 작동을 나타내는 모식도이다. DRM 인증서버(230)는 인터넷으로 사용자 컴퓨터와 연결되어 있으며, 사용자 컴퓨터에서는 사용자레벨에서 작동하는 것은 DRM 제어기(S52)와 응용프로그램(250)이 있으며, 시스템레벨에서 작동하는 것은 DRM 디바이스 드라이버(220)와 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템(240)이다. 암호화된 컨텐츠 패키지가 각각의 DRM 시스템 구성요소와 연계되어 작동하는 것을 살펴보면 다음과 같다. 먼저 사용자(500)가 암호화된 컨텐츠 패키지의 지정된 확장자(.cem) 파일을 열게 되면(S51), 자동으로 연결된 프로그램인 DRM 제어기(210)가 구동된다. DRM

제어기(210)는 암호화된 컨텐츠 패키지의 헤더 정보를 분석(S52)하여 파일이름 및 파일 크기, 서버정보, 컨텐츠 정보 등을 수집하여 분석하게 된다. 그 후 DRM 제어기(210)는 DRM 인증서버(230)와 연계하여 상술한 바와 같은 응용프로그램 인증 및 사용자 인증을 수행하여 라이센스 파일을 획득(S53)하게 된다. DRM 제어기가 분석한 컨텐츠 패키지의 헤더 정보에 의해 암호화된 파일이름을 알 수 있으며, DRM 제어기는 파일이름의 확장자를 이용해 관련 응용프로그램(250)을 구동시킨다. 이에 따라 운영체제는 응용프로그램의 구동에 따른 프로세스 식별자(Process Identification Information)를 생성하면, DRM 제어기는 상기 식별자를 획득한 후 응용프로그램의 실행을 잠시 중지(S54)시킨다. DRM 제어기(210)는 라이센스 파일의 암호화키와 프로세스 식별자, 파일이름 등을 DRM 디바이스 드라이버(220)에 등록(S55)을 시켜둔다. 추가적으로 DRM 드라이버에는 나중에 설명할 파일열기가 수행될 때 파일핸들이 등록된다. 상기 각종 데이터의 등록과정 후 응용프로그램(250)이 다시 구동되어 파일 열기 및 열기, 닫기 명령 등을 수행할 때, DRM 디바이스 드라이버는 상기 파일입출력요청 메시지를 후킹하여 메시지의 발생, 변형, 삭제 등을 수행하며 이것은 도 6, 7, 8에서 자세히 설명할 것이다. 도 5에서는 읽기 과정을 수행할 때 필요한 과정을 자세히 설명할 것이다. 읽기 과정에서는 응용프로그램이 파일시스템에 파일옵셋과 파일길이를 요청(S56)하며, 이것은 각 응용프로그램마다 고유한 값을 가지게 된다. DRM 디바이스 드라이버(220)는 상기 응용프로그램이 요청한 파일옵셋과 파일길이를 후킹한 후, 암호화된 컨텐츠 패키지 형태에 맞추어 16바이트 단위로 파일옵셋과 파일길이의 메시지를 변형처리(S57)해주는 작업을 수행

하고 복호화작업을 수행할 버퍼메모리의 주소를 지정한다. 상기 변형된 파일옵셋과 파일길이에 맞게끔 파일시스템(240)에 파일데이터를 요청하고, 요청된 패키지의 데이터를 도 10에서 자세히 설명할 임시저장공간인 버퍼메모리에 로딩하게 된다. 상기 버퍼메모리에서 DRM 디바이스 드라이버는 암호화된 데이터를 라이센스 파일에 포함된 암호화키(Kc)를 이용해 복호화를 수행한 후, 원래 응용프로그램이 요청한 복호화된 파일옵셋과 파일길이의 데이터로 복원처리(S60)를 하여 응용프로그램에 전달(S61)해 준다.

<42> 본 발명에서의 암호화 방법은 Rijndael 알고리즘을 이용한 16바이트(128비트) 단위로 수행되었다. Rijndael 알고리즘은 벨기에의 암호학자인 Vincent Rijndael 교수가 Joan Daemen과 함께 만들어 낸 것으로, 암호화 알고리즘의 보안성 및 성능, 효율성, 적용성 등의 조화가 타 알고리즘에 비해 탁월한 장점이 있다. 본 발명에서는 Rijndael 알고리즘을 이용해 16바이트(128비트)로 암호화하였으나, 당연히 다른 알고리즘을 이용하거나 32바이트(256비트)등 다른 단위로 암호화시킬 수 있음은 자명한 일이다. 도 5에서 파일옵셋 및 파일길이의 메시지 변형과 데이터 복원이 필요한 이유는, 16바이트 단위로 암호화가 되었기 때문에 정확한 복호화를 위해서는 파일시스템에 16바이트 단위로 파일옵셋 및 파일길이의 데이터를 요청하여 복호화해 주어야 하기 때문이다. 각각의 응용프로그램마다 요청하는 파일옵셋과 파일길이가 모두 틀리기 때문에, DRM 디바이스 드라이버는 응용프로그램과 파일시스템의 중간에 위치하여 파일입출력요청 메시지를 실시간으로 후킹하여 응용프로램이 요청하는 파일옵셋 및 파일길이 형태로 암호화된 데이터를 복호화하고 다시 복원처

리를 해 주어야만 한다. 복호화 및 복원처리는 모두 시스템 레벨에서 작업이 수행되기 때문에 사용자 레벨에서의 응용프로그램은 실제로 DRM 디바이스 드라이버로부터 제공받는 파일데이터가 일반 데이터인지 DRM이 적용된 암호화된 데이터인지를 구분하지 못하게 된다. 또한 응용프로그램과 DRM 디바이스 드라이버 사이에서는 암호가 풀린 상태에서 데이터가 전송되므로, 만약 다른 드라이버가 DRM 드라이버보다 상단에 로딩이 된다면 보안상의 취약점이 발생한다. 따라서 완벽한 보안을 위해서 DRM 디바이스 드라이버는 운영체제에서 필요로 하는 각종 드라이버중의 최상위 레이어에 로딩되어야 한다. 이를 위해 DRM 디바이스 드라이버는 다른 디바이스 드라이버의 로딩을 감시하고 있다가 DRM 디바이스 드라이버위에 다른 디바이스 드라이버가 로딩되는 것을 감지하면 DRM 디바이스 드라이버는 동작을 멈추는 기능을 가지고 있다. 또한 도 9에서 설명이 될 DRM 디바이스 드라이버의 또 다른 기능중의 하나는 응용프로그램의 프로세스 종료 탐지(Process kill detect) 기능이 있다. 이것은 DRM 드라이버가 응용프로그램의 프로세스가 종료되는 것을 감시하고 있다가 종료 메시지를 탐지하면, 종료되는 응용프로그램의 프로세스 식별자와 관련한 모든 자료(파일이름, 암호화키 등)를 모두 삭제하고 DRM 제어기에 통보하게 되고 등록된 프로세스 식별자가 더 이상 없다면 DRM 디바이스 드라이버의 후킹 동작도 멈춤으로서 보안성능을 크게 향상 시킬 수 있게 된다.

<43> 도 6 및 도 7, 도 8, 도 9는 DRM 디바이스 드라이버(220)가 후킹하는 파일입출력 메시지가 열기(open), 읽기(read), 닫기(close) 명령일 때와 응용프로그램 종료 메시지를 탐지하는 기능에 관한 그림이다.

<44> 도 6은 암호화된 디지털 컨텐츠의 열기과정을 보여주는 흐름도이다. 먼저 응용프로그램(250)이 파일시스템(240)에 열기 명령을 내리면, 파일시스템에서 응용프로그램으로 올라가는 파일입출력요청 메시지를 후킹(601)하여 응용프로그램의 프로세스 식별자 등록여부를 확인(601)한다. 응용프로그램의 프로세스 식별자가 DRM 드라이버에 등록되어 있지 않다면 일반 데이터 파일을 여는 것이므로 응용프로그램으로 명령을 전달하고, 만약 응용프로그램의 프로세스 식별자가 등록되어 있다면 암호화된 컨텐츠 파일을 여는 것이므로 파일핸들(604)을 등록시킨 후 응용프로그램으로 명령을 전달하게 된다. 즉 DRM 디바이스 드라이버는 열기 명령일 때 파일입출력요청 메시지의 후킹(601)을 파일시스템의 후반부에서 실행하며 주요기능은 파일핸들의 등록(604)이다.

<45> 도 7은 암호화된 디지털 컨텐츠의 읽기 과정을 보여주는 흐름도이다. DRM 디바이스 드라이버는 응용프로그램이 읽기 명령을 내리면 파일입출력요청 메시지를 후킹(701)하여 응용프로그램의 프로세스 식별자 등록여부를 확인(702)한다. 식별자가 등록되어 있지 않다면 일반 데이터 파일이므로 파일시스템(240)으로 명령을 전달하고, 만약 식별자가 등록되어 있다면 파일핸들의 등록여부를 확인(703)하게 된다. 마찬가지로 파일핸들이 등록되어 있지 않으면 파일시스템으로 명령을 넘기고, 만약 파일핸들이 등록되어 있다면 응용프로그램에서 요구하는 파일옵셋 및 파일길이의 형식을 암호화된 패키지 데이터에 맞게끔 상기 메시지의 변형처리(704)를 해 준다. 그 후 복호화 작업과 복원작업을 위해 임시저장공간인 버퍼메모리를 지정(705)해주고 파일시스템(240)으로 명령을 전달한다. 파일시스템에서 만들어진 파일입출력요청 메시지를 다시 후킹(706)하여 변형된 파일옵셋 및 파일길이 만큼의 암호화 데이터를 상기 버퍼메모리에 로딩하여 암호화키를 이용해 복

호화(707)한다. 그후 복호화된 데이터를 원래 응용프로그램(250)이 요청한 값의 파일옵셋 및 파일길이로 복호화된 데이터를 복원(708)해 주고난 후, 이것을 버퍼메모리에 복사(709)하여 응용프로그램이 읽을 수 있도록 전달해 주게 된다. 상기와 같은 과정을 실시간으로 계속 반복하면서 다른 메시지가 전달될 때까지 암호화된 파일의 복호화를 수행한다. 본 발명에서는 DRM 디바이스 드라이버에서 파일입출력요청 메시지를 후킹하여 파일옵셋 및 파일길이를 변형 및 복원처리를 해 주기 때문에 응용프로그램은 읽기과정을 수행할 때 파일시스템으로부터 전달받는 데이터가 일반 데이터인지 암호화된 것인지 구별하지 못한다. 또한 버퍼메모리에서만 암호화 파일을 16바이트 단위의 조각난 데이터를 복호화하여 응용프로그램에 전달하기 때문에, 사용자가 무단으로 암호화된 파일을 복사하는 것이 원천적으로 봉쇄하게 된다. 결론적으로 DRM 디바이스 드라이버는 읽기 명령일 때 파일입출력요청 메시지의 후킹(701,706)은 파일시스템의 전반부와 후반부에서 모두 수행되며, 주요기능은 파일옵셋 및 파일길이의 메시지 변형 및 암호화파일의 복호화, 복호화된 데이터의 복원작업이다. 또한 DRM 디바이스 드라이버에 복호화 수단 뿐만아니라 암호화 수단을 더 포함하면, 암호화된 컨텐츠의 수정 및 편집, 재저장 등의 기능이 구현될 수 있으며, 이것은 본 발명의 기술적 사상을 이용하여 당업자라면 쉽게 구현할 수 있으므로 여기서는 자세한 설명은 생략한다.

<46> 도 8은 암호화된 디지털 컨텐츠의 닫기 과정을 보여주는 흐름도이다. 응용프로그램(250)이 닫기 명령을 파일시스템(240)에 내리면, 파일시스템에서 응용프로그램으로 전달되는 파일입출력요청 메시지를 후킹(801)하여 응용프로그램의 프로세스 식별자 등록여부를 확인(802)하고 난 후, 만약 식별자가 등록되어 있다면 파일핸들 유무를 확인(803)하

고 파일핸들이 존재한다면 파일핸들을 삭제(804)하고서 응용프로그램에 명령을 전달하게 된다.

<47> 도 9는 응용프로그램의 종료 과정을 보여주는 모식도이다. 사용자(500)가 응용프로그램(250)을 종료하는 명령을 내리면 운영체제(900)에 종료메시지가 전달되고, 상기 응용프로그램의 종료 메시지를 DRM 디바이스 드라이버(220)가 탐지하고, 종료되는 응용프로그램의 프로세스 식별자가 등록되어 있는 정보라면 상기 식별자와 관련한 모든 자료(파일이름, 암호화키 등)를 삭제하고 DRM 제어기(210)에 종료메시지를 통보하고 DRM 디바이스 드라이버 상에 등록된 응용프로그램의 프로세스 식별자가 더 이상 없다면 후킹 동작도 멈추게 된다.

<48> 본 발명의 기술적 사상을 이용하면 디바이스 드라이버 단계에서의 파일입출력요청 메시지의 후킹을 수행함으로서 응용프로그램의 열기, 읽기, 닫기 뿐만 아니라, 쓰기, 저장, 복사, 인쇄 등의 일반적 기능을 온(On)/오프(Off) 제어를 할 수 있음은 당업자라면 쉽게 추측할 수 있을 것이다. 또한 본 발명의 디바이스 드라이버 단계의 시스템 제어기술을 사용하면 매크로형태 및 첨부파일에 포함되어 유포되는 e-mail 바이러스의 피해를 방지할 수 있도록, 메일관리 프로그램을 디바이스 드라이버 단계에서 제어하여 첨부파일의 수행을 제한하거나 수행이 되었다고 하더라도 내부자료에 접근하지 못하도록 할 수도 있다.

<49> 도 10과 도 11은 암호화된 디지털 컨텐츠의 복호화 과정과 복호화된 데이터의 복원과정을 보다 상세히 설명한다.

<50> 도 10은 암호화된 디지털 컨텐츠의 복호화 과정을 보여주는 모식도이다. 일반적인 디지털 데이터는 파일헤더(1020)와 데이터(1030)로 구분되어 있다. 따라서 디지털 컨텐츠를 암호화할 때는 특정한 암호화키를 이용해서 파일헤더(1020)와 데이터(1030)를 암호화하게 되며, 파일헤더 앞에 암호화되지 않은 디지털 컨텐츠 패키지의 헤더(1010)를 붙이게 된다. 디지털 컨텐츠 패키지의 헤더(1010)는 도 5에서 설명한 것과 같이 사용자가 지정된 확장자(.cem)의 파일을 선택하여 열면, 자동으로 DRM 제어기(210)가 구동하여 패키지의 헤더를 분석하여 파일이름 및 파일크기, 서버정보, 컨텐츠정보, 패키지 버전 등의 복호화를 위한 정보를 읽어 들이는데 사용하게 된다. 전술한 바와 같이 응용프로그램이 파일시스템에 요청하는 파일옵셋 및 파일길이 메시지를 DRM 디바이스 드라이버에서 후킹 및 메시지 변형하여 파일시스템에 전달하는 과정은 본 그림에서 생략되어 있고, 복호화 및 복호화된 데이터의 복원과정을 도시하고 있다. 변형된 파일옵셋 및 파일길이 메시지에 해당하는 암호화된 데이터(1040)가 이미 지정되어 있는 버퍼메모리(1000)로 전달되고, DRM 디바이스 드라이버(220)는 버퍼메모리에서 암호화키를 이용해 복호화하며, 상기 복호화된 데이터를 원래 응용프로그램이 요청한 파일옵셋 및 파일길이 값으로 복원하여 응용프로그램에 전달하게 된다. 본 그림에서는 생략되어 있지만 디지털 컨텐츠 패키지의 암호화를 하나의 암호화키를 이용하는 방법 또는 보안수준을 높이기 위해 여러개의 암호화키를 이용해서 암호화 및 복호화를 할 수도 있다. 예를 들면 암호화해야할 디지털 컨텐츠의 용량이 50메가바이트이라면, 10메가바이트씩 5개의 암호화키를 이용해

서 암호화를 수행하고 관련 정보를 컨텐츠 패키지의 헤더와 라이센스 정보파일에 기록하여 복호화를 수행함으로서 보안수준을 한층 더 높일 수 있다.

<51> 도 11은 암호화된 디지털 컨텐츠의 파일옵셋과 파일길이를 처리하는 과정을 보여주는 모식도이다. 본 발명의 실시예에서는 Rijndael 알고리즘을 사용하기 때문에 16바이트(128비트) 단위로 암호화 및 복호화가 이루어지며, 그림에서 암호화된 데이터 블록(1110)들은 동일하게 16바이트로 암호화 된 것을 보여준다. 응용프로그램이 요청한 실제 파일옵셋 및 파일길이에 해당하는 데이터블록(1120)이 16바이트 단위의 데이터블록 두개(1110a와 1110b)에 걸쳐 있다면, 상기 암호화된 두개의 데이터블록에 맞게끔 파일옵셋 및 파일길이 메시지를 변형하여서 파일시스템에 전달하게 되며 이 과정은 본 그림에서 생략되어 있다. 따라서 변형된 파일옵셋과 파일

길이 메시지에 해당하는 두개의 데이터블록(1110a와 1110b)을 모두 버퍼메모리(1000)에 로딩하여, DRM 디바이스 드라이버에 등록되어 있는 암호화키를 이용하여 복호화하고 난 후 원래 응용프로그램(250)이 요청했던 파일옵셋과 파일길이 형태의 데이터로 복원처리하여 만들어진 데이터블록(1120)을 응용프로그램(250)에 전달하게 된다. 그 후 응용프로그램이 요청하는 다음순서의 파일데이터에 해당하는 임의의 크기인 데이터블록(1121)도 상기와 똑같은 과정을 거친 후 응용프로그램에 전달하는 과정을 거치게 된다. 본 과정은 실시간으로 버퍼메모리상에서 일어나기 때문에 도 2에서 설명한 바와 같이 컨텐츠 배포자(260)의 웹서버 및 FTP 서버로부터 다운로드(S26)하여 저장된 암호화된 컨텐츠 패키지 뿐만 아니라, HTTP 프로토콜을 이용해서 다운로드 과정과 동시에 HTTP 스트리밍 서비스도 가능하게 된다. 이것은 본 발명의 중요한 특징 중의 하나로서 기존의 DRM 시스템이 일반적으로 다운로드가 완료된 암호화된 컨텐츠에 대해서만 적용할 수 있는데 비해서, 본 발명은 다운로드를 완료한 컨텐츠 뿐만 아니라 다운로드 중에 HTTP 스트리밍 서비스도 가능하게 된다. 이것은 온라인 강의나 인터넷영화, 동영상파일등의 대용량의 디지털 컨텐츠에 DRM 시스템을 적용할 경우 다운로드를 받는 시간동안 사용자가 불편하게 기다리던 불편을 완전히 해소한 매우 유리한 장점을 가지게 된다. 또한 본 발명을 통해 웹서버를 통한 HTTP 스트리밍 서비스가 다운로드와 동시에 이루어지므로 컨텐츠 배포자(260)가 DRM을 적용한 디지털 컨텐츠의 스트리밍 서비스를 위해 필요한 MMS (Microsoft windows Media Server) 서버 등의 구입 및 운영 비용을 절감할 수 있는 장점을 가진다.

<52> 도 12는 암호화된 디지털 컨텐츠 패키지 파일의 데이터 구조를 보여주는 모식도이다. 패키지의 헤더(1010)에는 엔코딩 헤더(encoding header), 패키지 버전(package version), 사이트 아이디(site ID), 서비스아이템 아이디(service item ID), IP 주소(IP address), 포트정보(port inforamtion), 하드웨어 프래그(hardware flag), 파일크기(file size), 파일이름(file name), 암호키의 총 숫자(total key count), 엔코팅 크기(endoding size) 등의 정보가 들어간다. 여기서 IP 주소와 포트정보, 파일이름은 각 디지털 컨텐츠 마다 크기가 다르지만, 나머지는 모두 정해진 용량 값으로 패키지 헤더를 구성할 수 있다. 패키지 헤더의 구성내용은 얼마든지 컨텐츠 공급자(Contents Provider)나 컨텐츠 배포자가 조정할 수 있을 것이다. 패키지 헤더(1010)는 암호화되지 않으며 실제 암호화되는 것은 원래 디지털 컨텐츠의 파일헤더(1020)와 파일데이터(1030)가 된다. 상기 파일헤더(1020)는 일반적인 컴퓨터 파일에서 앞부분에 위치하며 데이터의 길이라든가 파일의 다른 특성들을 기술하고 있는 필드이며 본 발명에서 보여주는 것은 가장 일반적인 디지털 데이터의 형식이며 얼마든지 형식이 바뀌어 질 수가 있다.

<53> 도 13은 라이센스 파일의 데이터 구조를 보여주는 모식도이다. 라이센스 파일은 도 3에서 전술한 바와 같이 응용프로그램 인증 및 사용자 인증을 거친 후 DRM 인증서버(230)가 사용자 컴퓨터의 DRM 제어기(210)에 온라인으로 전달할 수도 있고, 오프라인으로 라이센스 정보파일(300)을 제공할 수도 있다. 라이센스 정보 파일에는 라이센스 플래그(license flag), 사용기간의 시작 및 종료일자(start & end date), 사용횟수정보(total & current count), 인쇄횟수(total print), 사용컴퓨터의 숫자(total and current PC), 단일키 및 복수키 암호화 정보(total and current Kc index, Kc), 서비스아이템 이름

(service item name) 등의 정보가 컨텐츠 공급자나 배포자의 요구에 맞게 제작할 수 있는 것은 당업자라면 주지의 사실이다. 상기에서 사용기간의 시작 및 종료일자는 컨텐츠 사용자가 기간연장의 목적으로 사용자 컴퓨터의 시간조정을 하는 것을 막기 위해 마지막으로 디지털 컨텐츠를 이용한 시간에 대한 정보를 암호화하여 사용자 컴퓨터의 레지스트리에 기록해 두고, 다음에 이용할 때 시간정보를 비교하여 사용기간의 불법연장을 막을 수 있다. 또한 사용횟수에 관한 정보는 컴퓨터의 카운터를 이용하여 자동으로 체크하도록 구성되어 있으며, 사무실과 가정 등에서 사용할 수 있는 컴퓨터의 숫자 등을 제어할 수 있는 라이센스에 관한 정보를 DRM 제어기에 제공하게 된다.

<54> 도 14는 본 발명의 일실시예에 따른 DRM이 적용된 HTTP 스트리밍을 보여주는 동영상강의 화면의 예시도이다. HTTP 프로토콜을 사용하는 웹서버를 이용하여 디지털 컨텐츠를 다운로드 받을 때, 다운로드와 동시에 HTTP 스트리밍이 이루어지는 것을 보여주고 있다. 동영상 강의 화면의 아래부분에 약간 희게 나타난 경계부분이 실제 다운로드가 진행되는 상태를 보여주는 것이며, 작은 직사각형의 상태바(status bar)는 현재 스트리밍이 진행되는 위치를 보여준다. 사용자는 HTTP 스트리밍만을 이용할 것인지, HTTP 스트리밍 및 다운로드 서비스를 동시에 이용할 것이지, 또한 디지털 컨텐츠의 저장위치와 파일이름을 결정할 수 있다. 따라서 완벽한 디지?? 컨텐츠의 정보보호가 이루어진 상태에서 다운로드와 동시에 스트리밍을 진행할 수 있음을 알 수 있다.

<55> 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러가지로 치환, 변형 몇 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 한정되는 것이 아니다.

【발명의 효과】

<56> 본 발명에서 제안한 디지털 컨텐츠의 정보보호 방법 및 시스템은 일반 응용프로그램의 시스템 레벨에서의 디바이스 드라이버 제어기술을 사용함으로서, 전용뷰어프로그램의 개발없이 기존의 다양한 응용프로그램을 사용함으로서 현재 통용되고 있는 모든 컨텐츠 파일형식에 적용되는 일반적인 DRM 시스템을 구축할 수 있도록 해줌으로서 향후 새로운 종류의 컨텐츠에 능동적으로 대응할 수 있다.

<57> 상기 디지털 컨텐츠를 이용하기 위한 일반 응용프로그램의 등록 및 관리, 인증 등은 온라인으로 DRM 인증서버 및 오프라인으로 라이센스 파일을 이용하여 손쉽게 관리 및 업그레이드할 수 있다.

<58> 또한 본 발명의 디지털 컨텐츠 정보보호 시스템은 일반 문서(아래아한글, MS워드, 훈민정음 등), MS 오피스(파워포인트, 엑셀, 엑세스 등), Media player, 이미지, 동영상강의, 음악 등의 모든 파일 형식을 지원하며, 상기 상용 프로그램은 응용프로그램의 인증을 수행하는 DRM 인증서버에 손쉽게 등록하여 사용할 수 있다.

<59> 본 발명의 시스템을 이용하면 중요한 문서나 컨텐츠를 보호하기 위해서 임의의 파일에 대한 접근 허용을 시스템 단계에서 제어함으로서, 허가받지 않은 사람들에 대한 접근제

어를 할 수 있다. 또한 특정파일을 이용하는 응용프로그램에 대하여 시스템단계에서의 다양한 파일조작을 통한 새로운 서비스를 개발할 수 있다.

<60> 또한 디바이스 드라이버 단계에서의 파일입출력요청 메시지의 후킹을 수행함으로서 응용프로그램의 열기, 읽기, 닫기 뿐만 아니라, 쓰기, 저장, 복사, 인쇄 등의 일반적 기능을 온(On)/오프(Off) 제어를 할 수 있다.

<61> 또한 본 발명의 디바이스 드라이버 단계의 시스템 제어기술을 사용하면 매크로형태 및 첨부파일에 포함되어 유포되는 e-mail 바이러스의 피해를 방지할 수 있도록, 메일관리 프로그램을 디바이스 드라이버 단계에서 제어하여 첨부파일의 수행을 제한하거나 수행이 되었다고 하더라도 내부자료에 접근하지 못하도록 할 수 있다.

<62> 본 발명은 특정 운영체제에 국한되는 것이 아니며, 윈도우의 다른 버젼, 리눅스, 유닉스 등의 기타 다른 운영체제에서도 동일한 기술적 사상 내에서 당업자라면 다양한 변형을 손쉽게 만들어 낼 수 있을 것이다. 또한 본 발명은 컴퓨터 프로그램으로 제작될 수도 있고, 제작된 컴퓨터 프로그램은 기록매체에 저장되거나, 전송매체에 의해 전송될 수도 있다.

【특허청구범위】

【청구항 1】

디지털 컨텐츠의 정보보호 시스템에 있어서,

온라인 또는 오프라인으로 컨텐츠 배포자(260)로부터 제공받아 사용자 컴퓨터에 저장된 암호화된 컨텐츠 패키지(240)를 선택하여 열면 자동으로 DRM 제어기(210)가 구동하여 컨텐츠 패키지 헤더(1010) 속에 포함된 파일이름 및 파일크기, 서버정보, 컨텐츠 정보 등을 수집하여 분석하는 정보분석수단과,

상기 패키지 헤더의 정보분석을 바탕으로 DRM 제어기가 인터넷으로 연결된 DRM 인증서버(230)로 부터 응용프로그램 인증 및 사용자 인증을 수행하는 인증수단과,

상기 인증결과를 바탕으로 DRM 제어기가 획득한 라이센스 파일을 이용하여 컨텐츠의 사용기간 또는 사용횟수, 사용가능한 컴퓨터의 숫자 등의 관리를 하는 라이센스 관리수단과,

상기 암호화된 컨텐츠 패키지를 볼 수 있는 응용프로그램의 기동 및 제어, 종료 등을 수행하는 제어수단과,

DRM 디바이스 드라이버(220)가 응용프로그램과 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템간의 열기, 읽기, 닫기, 종료 등의 파일입출력요청 메시지를 가로채는 디바이스 드라이버 단계의 후킹 수단과,

상기 디바이스 드라이버 단계의 후킹 정보인 응용프로그램이 파일시스템에 요청한 파일옵셋 및 파일길이의 정보변형수단과,

상기 변형된 파일옵셋 및 파일길이의 정보를 바탕으로 암호화된 컨텐츠 패키지의 데이터를 버퍼메모리로 가져와서 복호화하는 복호화 수단과,

상기 버퍼메모리에서 복호화된 컨텐츠 패키지의 데이터를 응용프로그램이 요청했던 파일옵셋 및 파일길이 형태로 복원하는 복원수단과,

상기 복호화되어 복원된 컨텐츠 패키지의 데이터를 응용프로그램에 전달하는 전달수단을 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【청구항 2】

제 1항에 있어서,

상기 응용프로그램 인증 및 사용자 인증이 DRM 인증서버에 의해 온라인으로 이루어지는 것 대신에, CD 또는 디스켓, 기타 저장장치를 통해 제공된 라이센스 파일을 이용해 오프라인으로 이루어지는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【청구항 3】

제 1항에 있어서,

상기 사용자 인증은 DRM 인증서버와 연동된 컨텐츠 배포자의 웹서버 또는 FTP 서버 등에서 수행한 사용자 로그인 정보를 이용하여 자동으로 DRM 인증서버에서 수행되는 인증수단을 더 포함한 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【청구항 4】

제 1항에 있어서,

상기 암호화된 컨텐츠 패키지는 하나의 암호화키 또는 여러개의 암호화키를 이용하여 암호화 및 복호화를 수행하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【청구항 5】

제 1항에 있어서,

상기 DRM 디바이스 드라이버가 운영체제에서 필요한 각종 디바이스 드라이버중 최상위 레이어에 로딩될 수 있도록, 다른 디바이스 드라이버가 로딩되는 것을 감지하면 DRM 디바이스 드라이버의 동작을 멈추게 하는 디바이스 드라이버 감시수단을 더 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【청구항 6】

제 1항 내지 제 5항 중 어느 한 항에 있어서,

상기 암호화된 컨텐츠 패키지는 사용자 컴퓨터에 저장된 것 대신에 컨텐츠 배포자로부터 사용자 컴퓨터로 다운로드 받아 저장하는 것과 동시에 HTTP 스트리밍으로 컨텐츠를 볼 수 있는 수단을 더 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【청구항 7】

제 1항 내지 제 6항 중 어느 한 항에 있어서,

상기 응용프로그램이 읽어들인 복호화된 디지털 컨텐츠의 데이터를 수정 또는 편집하여 다시 저장할 수 있도록 DRM 디바이스 드라이버에 암호화 수단을 더 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【청구항 8】

디지털 컨텐츠의 정보보호 방법에 있어서,

온라인 또는 오프라인으로 컨텐츠 배포자(260)로부터 제공받아 사용자 컴퓨터에 저장된 암호화된 컨텐츠 패키지(240)를 사용자가 선택하여 열면 자동으로 DRM 제어기(210)가 구동하는 단계(S51);

상기 DRM 제어기가 컨텐츠 패키지의 헤더(1010) 속에 포함된 파일이름 및 파일크기, 서버정보, 컨텐츠 정보 등을 수집하여 분석하는 단계(S52);

상기 패키지 헤더의 정보분석을 바탕으로 DRM 제어기가 인터넷으로 연결된 DRM 인증서버(230)로부터 응용프로그램 인증 및 사용자 인증을 수행하여 라이센스 파일의 정보를 획득하는 단계(S53);

DRM 제어기가 응용프로그램에게 프로세스 식별자를 생성한 후 응용프로그램의 실행을 잠시 중지하는 단계(S54);

DRM 제어기가 DRM 인증서버로부터 획득한 라이센스 및 응용프로그램 인증정보를 DRM 디바이스 드라이버에 등록시키는 단계(S55);

상기 잠시 중지된 응용프로그램이 다시 구동하여 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템에 파일옵셋과 파일길이를 요청하는 파일입출력요청 메시지를 DRM 디바이스 드라이버에서 후킹하는 단계(S56);

상기 후킹된 파일입출력요청 메시지의 파일옵셋과 파일길이를 암호화된 컨텐츠 패키지의 형태에 맞추어 변형해주는 단계(S57);

상기 변형된 파일옵셋과 파일길이에 맞게끔 암호화된 컨텐츠 패키지의 데이터를 임시저장공간인 버퍼메모리에 로딩하여 복호화하고 원래 응용프로그램이 요청한 파일옵셋과 파일길이에 맞게끔 복호화된 컨텐츠 패키지의 데이터를 복원하는 단계(S60); 및

상기 복원된 파일옵셋과 파일길이에 맞게끔 복호화된 컨텐츠 패키지의 데이터를 응용프로그램에 전송하는 단계(S61)를 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 방법.

【청구항 9】

제 8항에 있어서,

상기 DRM 제어기가 인터넷으로 연결된 DRM 인증서버로부터 사용자 인증을 수행할 때 사용자의 패스워드 정보노출을 막아주는 양방향세션인증 방법을 사용하는 단계를 더 포함하는 것 특징으로 하는 디지털 컨텐츠의 정보보호 방법.

【청구항 10】

제 8항에 있어서,

상기 DRM 디바이스 드라이버가 운영체제에서 필요한 각종 디바이스 드라이버중 최상위 레이어에 로딩될 수 있도록, 다른 디바이스 드라이버가 로딩되는 것을 감지하면 DRM 디바이스 드라이버의 동작을 멈추는 단계를 더 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 방법.

【청구항 11】

제 8항에 있어서,

상기 파일입출력요청 메시지의 후킹하는 단계에서 복호화된 데이터를 복원하여 전달하는 단계 중 어느 단계에서나, DRM 디바이스 드라이버가 응용프로그램의 종료메시지를 탐지하면 등록된 프로세스 식별자와 관련한 모든 자료를 삭제하고 DRM 제어기에 종료메시지를 통보하고 드라이버 상에 더 이상 등록된 식별자가 없다면 후킹 동작을 멈추는 단계를 더 포함하는 디지털 컨텐츠의 정보보호 방법.

【청구항 12】

제 8항 내지 제 10항 중 어느 한 항에 있어서,

상기 응용프로그램이 읽어들인 복호화된 디지털 컨텐츠의 데이터를 수정 또는 편집하여 다시 저장할 수 있도록 DRM 디바이스 드라이버에 암호화 단계를 더 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 방법.

【청구항 13】

디지털 컨텐츠의 정보보호 시스템에 있어서,

온라인 또는 오프라인으로 컨텐츠 배포자로부터 제공받아 사용자 컴퓨터에 저장된 암호화된 컨텐츠 패키지를 사용자가 선택하여 열면 자동으로 DRM 클라이언트 프로그램(200)이 구동하여 컨텐츠 패키지의 헤더 정보를 분석하는 기능;

상기 정보분석을 바탕으로 DRM 클라이언트 프로그램이 인터넷으로 연결된 DRM 인증서버로 부터 응용프로그램 및 사용자 인증을 수행하는 기능;

상기 인증결과를 바탕으로 라이센스를 획득하여 라이센스를 관리하는 기능;

상기 DRM 클라이언트 프로그램이 상기 컨텐츠 패키지를 볼 수 있는 응용프로그램의 기동 및 제어, 종료 등을 제어하는 기능;

상기 응용프로그램과 파일시스템간의 파일입출력요청 메시지를 디바이스 드라이버 단계에서 가로채는 후킹기능;

상기 후킹 정보의 파일옵셋 및 파일길이를 변형하는 정보변형 기능;

상기 변형된 파일옵셋 및 파일길이를 바탕으로 암호화된 컨텐츠 패키지의 데이터를 버퍼메모리로 가져와서 복호화하는 기능;

상기 버퍼메모리에서 복호화된 컨텐츠 패키지의 데이터를 응용프로그램이 요청했던 파일옵셋 및 파일길이 형태로 복원하는 기능; 및

상기 복호화되어 복원된 컨텐츠 패키지의 데이터를 응용프로그램에 전달하는 전달기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【청구항 14】

제 13항에 있어서,

상기 암호화된 컨텐츠 패키지는 사용자 컴퓨터에 저장된 것 대신에, 컨텐츠 배포자의 웹 서버로부터 사용자 컴퓨터로 다운로드 받아 저장하는 것과 동시에 HTTP 스트리밍으로 컨텐츠를 볼 수 있는 기능을 더 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

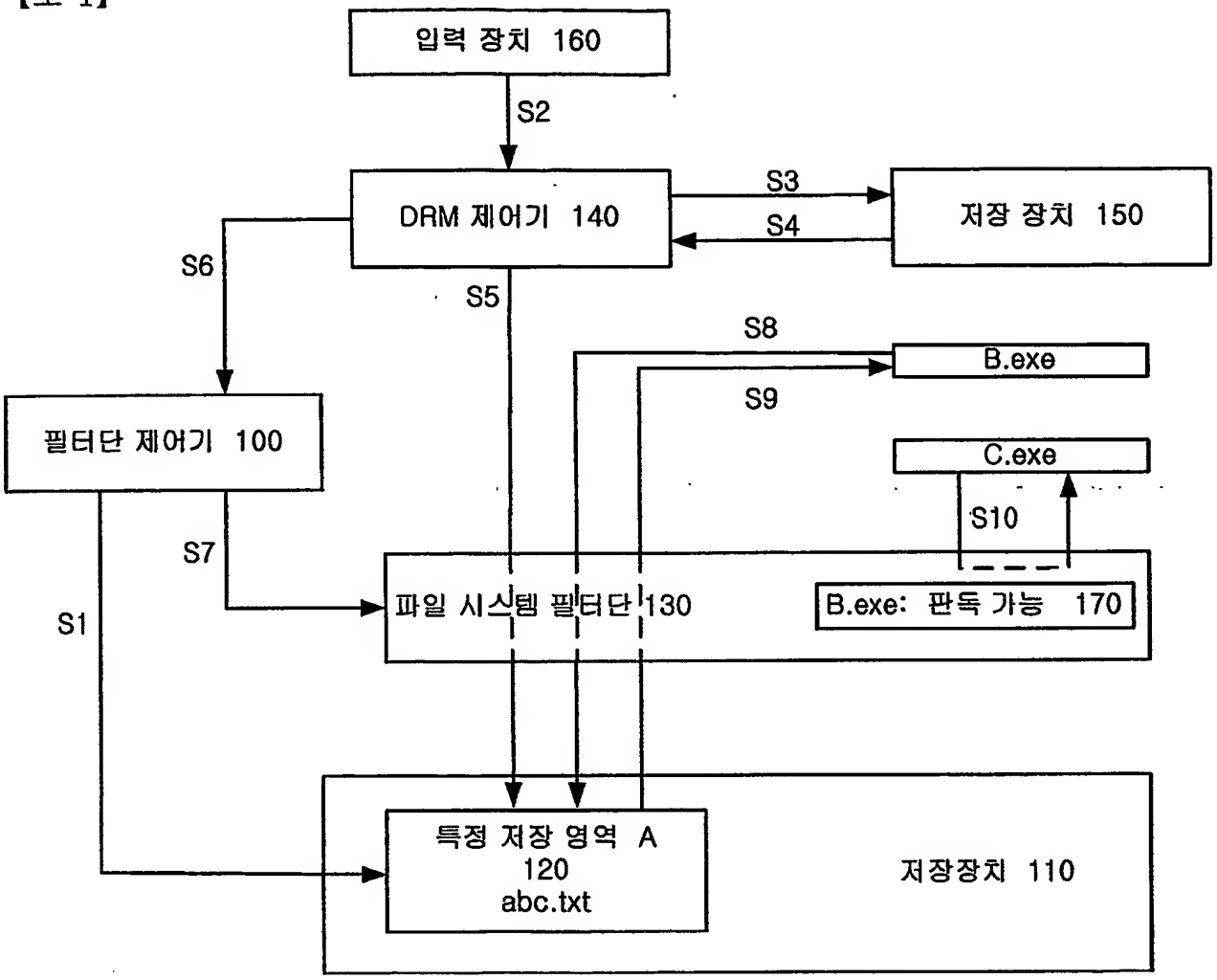
【청구항 15】

제 13항에 있어서,

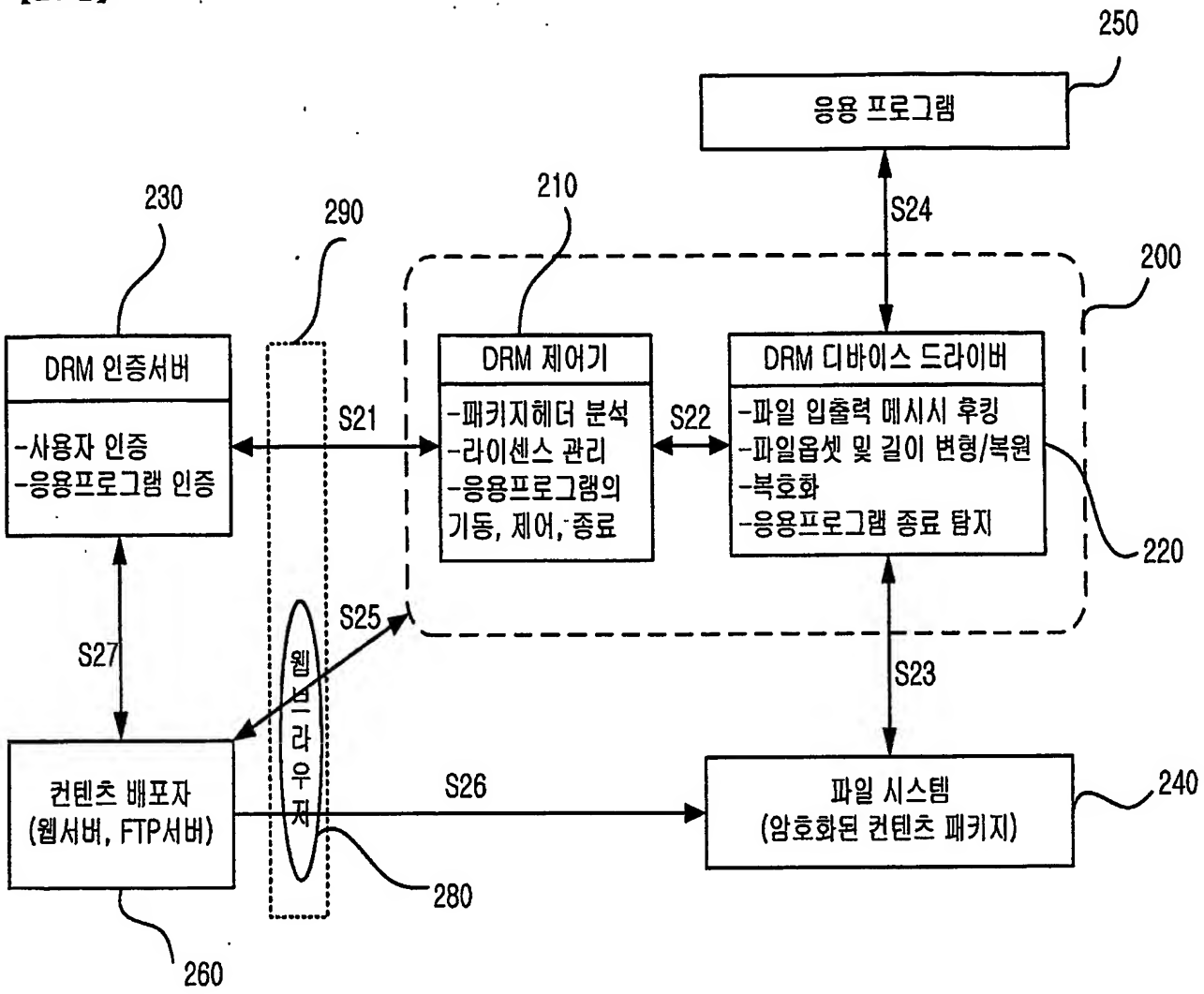
상기 응용프로그램이 읽어들인 복호화된 디지털 컨텐츠의 데이터를 수정 또는 편집하여 다시 저장할 수 있도록 DRM 디바이스 드라이버에 암호화 기능를 더 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

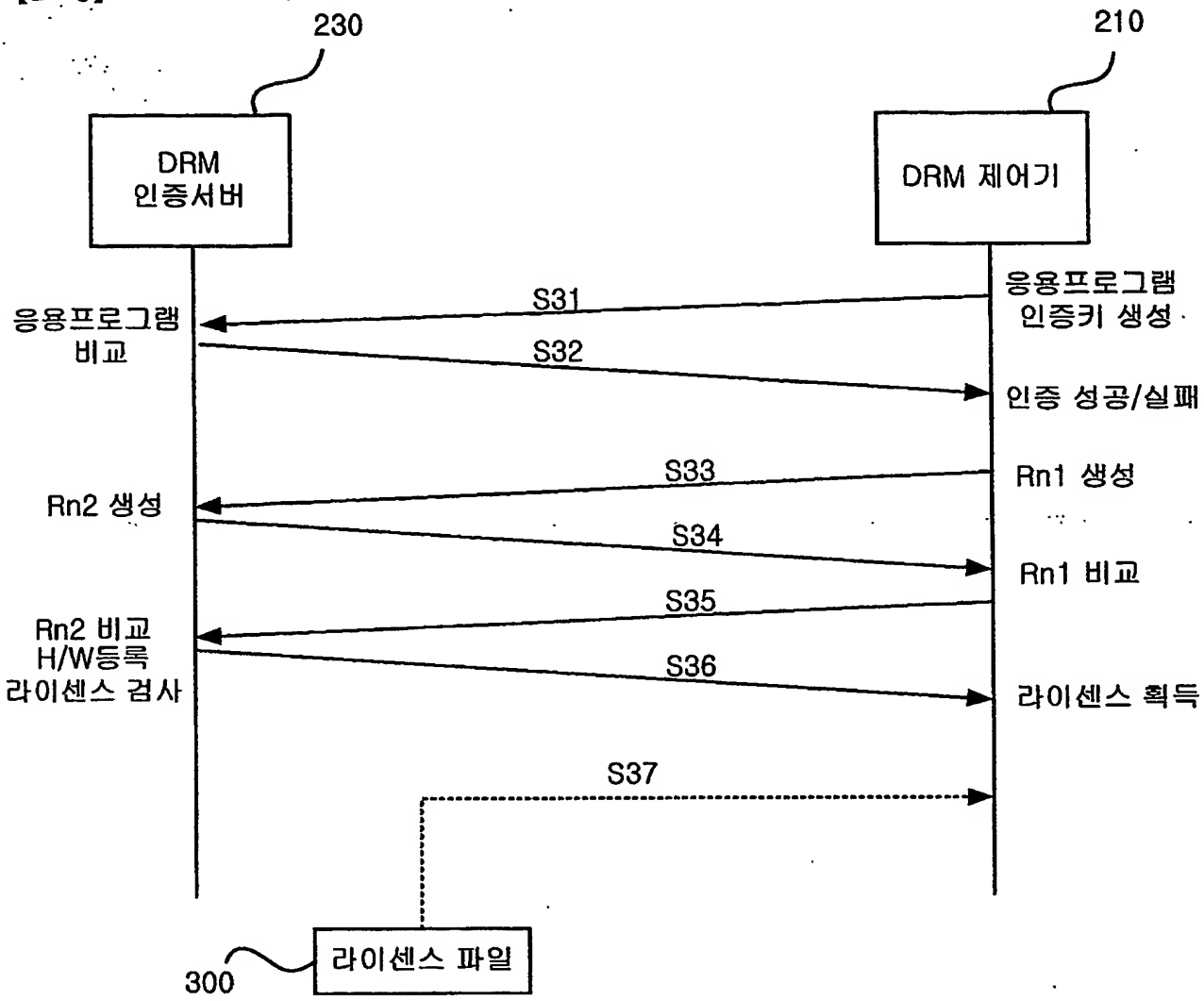
【도 1】


입력 장치 160
S2
DRM 제어기 140
S3
S4
저장 장치 150
S6
S5
S8
B.exe
S9
필터단 제어기 100
C.exe
S10
S7
S1
파일 시스템 필터단 130
B.exe: 판독 가능 170
특정 저장 영역 A
120
abc.txt
저장장치 110

【도 2】


250
응용 프로그램
S24
230
290
210
200
DRM 인증서버
-사용자 인증
-응용프로그램 인증
S21
DRM 제어기
-패키지헤더 분석
-라이센스 관리
-응용프로그램의 기동, 제어, 종료
S22
DRM 디바이스 드라이버
-파일 입출력 메시지 후킹
-파일옵셋 및 길이 변형/복원
-복호화
-응용프로그램 종료 탐지
220
S25
S27
S23
웹브라우저
컨텐츠 배포자
(웹서버, FTP서버)
S26
파일 시스템
(암호화된 컨텐츠 패키지)
240
280
260

【도 3】


230
210
DRM
인증서버
DRM 제어기
응용프로그램
인증키 생성
S31
응용프로그램
비교
S32
인증 성공/실패
S33
Rn1 생성
Rn2 생성
S34
Rn1 비교
S35
Rn2 비교
H/W등록
라이센스 검사
S36
라이센스 획득
S37
300
라이센스 파일

【도 4】

MEDIA KEEPER

Home , Back

: Level : Site : Member : Item : License : User PC : Viewer : Report : Account : Log

관리자 사이트 님 로그인 하셨습니다. Media Keeper [DRM 관리자] 입니다.

Viewer List

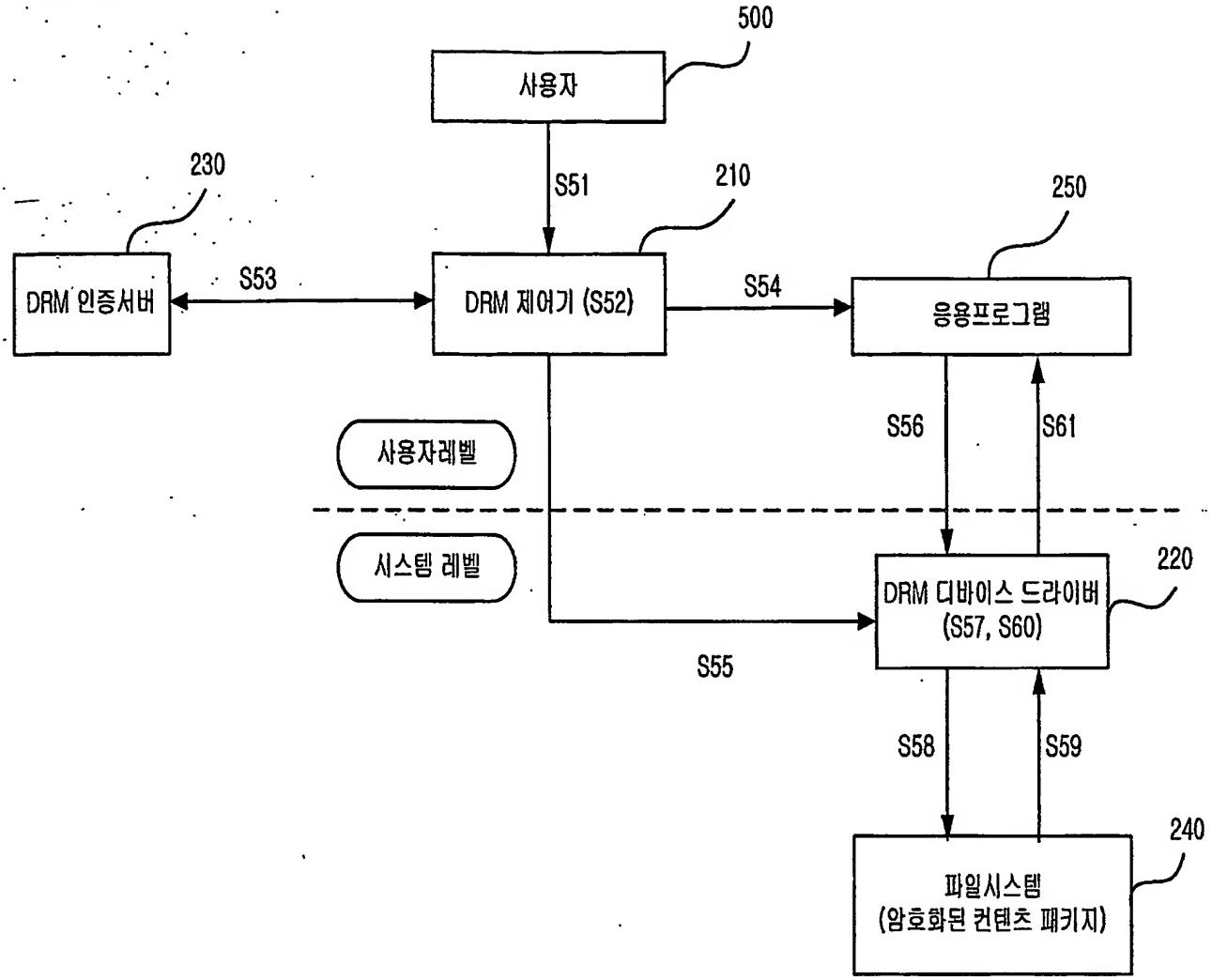
- 사용 가능한 Viewer를 등록 및 관리 합니다.
- H/W 인증뿐만 아니라 Viewer(S/W) 인증을 통하여 사용자로 하여금 허가된 프로그램 사용할수 있게 합니다.
- 등록 : 오른쪽 아래의 [Viewer 등록]을 누루면 새로운 Viewer 등록 합니다.
- 수정 : 기능 항목의 [E] 를 클릭·하면 해당 Viewer를 수정를 합니다.
- 삭제 : 기능 항목의 [D] 를 클릭·하면 해당 Viewer를 삭제를 합니다.

총 14 개의 인증된 프로그램이 등록 되어 있습니다

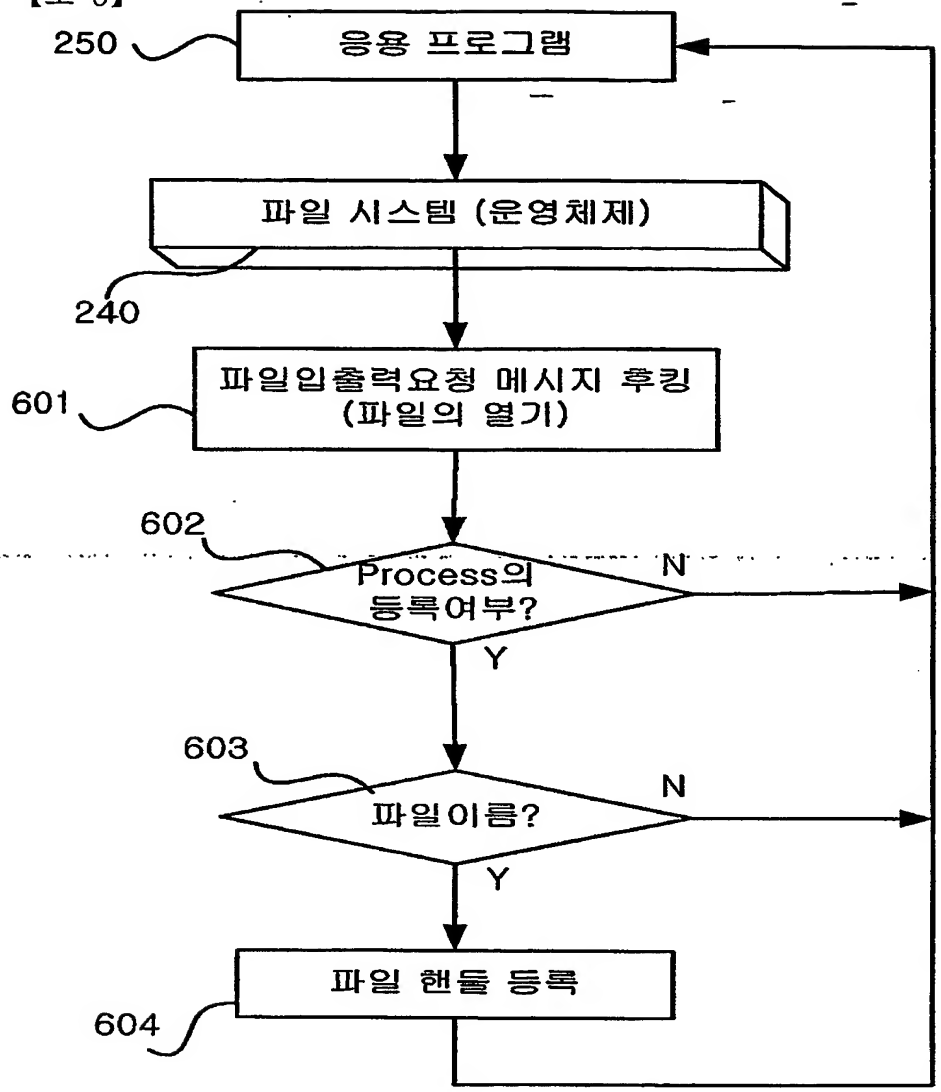
번호	인증된 프로그램	인증키	설명	용량	기능
17	[cyber] 98 Media Player 7.01	7203000000070710F	Windows Media Player 7.01	348,432	E / D
6	Acrobat Reader 4.0	0076727276070F07	Win 98/ME/NT/2000 [.pdf]	2,334,208	E / D
7	Acrobat Reader 5.0	7003000000777276	Win 98/ME/NT/2000 [.pdf]	3,870,784	E / D
3	Active Tutor 2.7.4.0	0071750500710473	Win 98/ME/NT/2000 [.apk]	438,272	E / D
5	Aikon 1.6.0.0	0205000104720107	Win 98/ME/NT/2000 [.adf]	24,576	E / D
2	GVA 2.00.0.2208	0071700400000000	Win 98/ME/NT/2000 [.gdb]	2,285,568	E / D
19	http 스트리밍 뷰어	00770077007F0077	HTTP 스트림을 위한 전용 프로그램입니다.	462,848	E / D
4	Live Share 1.5	0000000000000000	Win 98/ME/NT/2000 [.nsi]	1,240,057	E / D
16	Media Keeper Streamming Viewer	00770077007F0077	HTTP 스트림을 위한 전용 프로그램입니다.	507,904	E / D
8	Quick Time 5.02	0077050700737103	Win 98/ME/NT/2000 [.mov]^^	1,043,968	E / D
10	Windows Media Player 6.4	0075700000000000	Win 98/NT [.asf .avi .mov .mpeg .mpg .wmv]	4,880	E / D
12	Windows Media Player 6.4	0075700000000000	Win ME [.asf .avi .mov .mpeg .mpg .wmv]	12,288	E / D
13	Windows Media Player 6.4	0075700000000000	Win 2000 [.asf .avi .mov .mpeg .mpg .wmv]	5,120	E / D
14	Windows Media Player 7.1	0071087E0070717E	Win 98/ME/NT/2000 [.asf .avi .mov .mpeg .mpg .wmv]	348,160	E / D

Viewer 등록

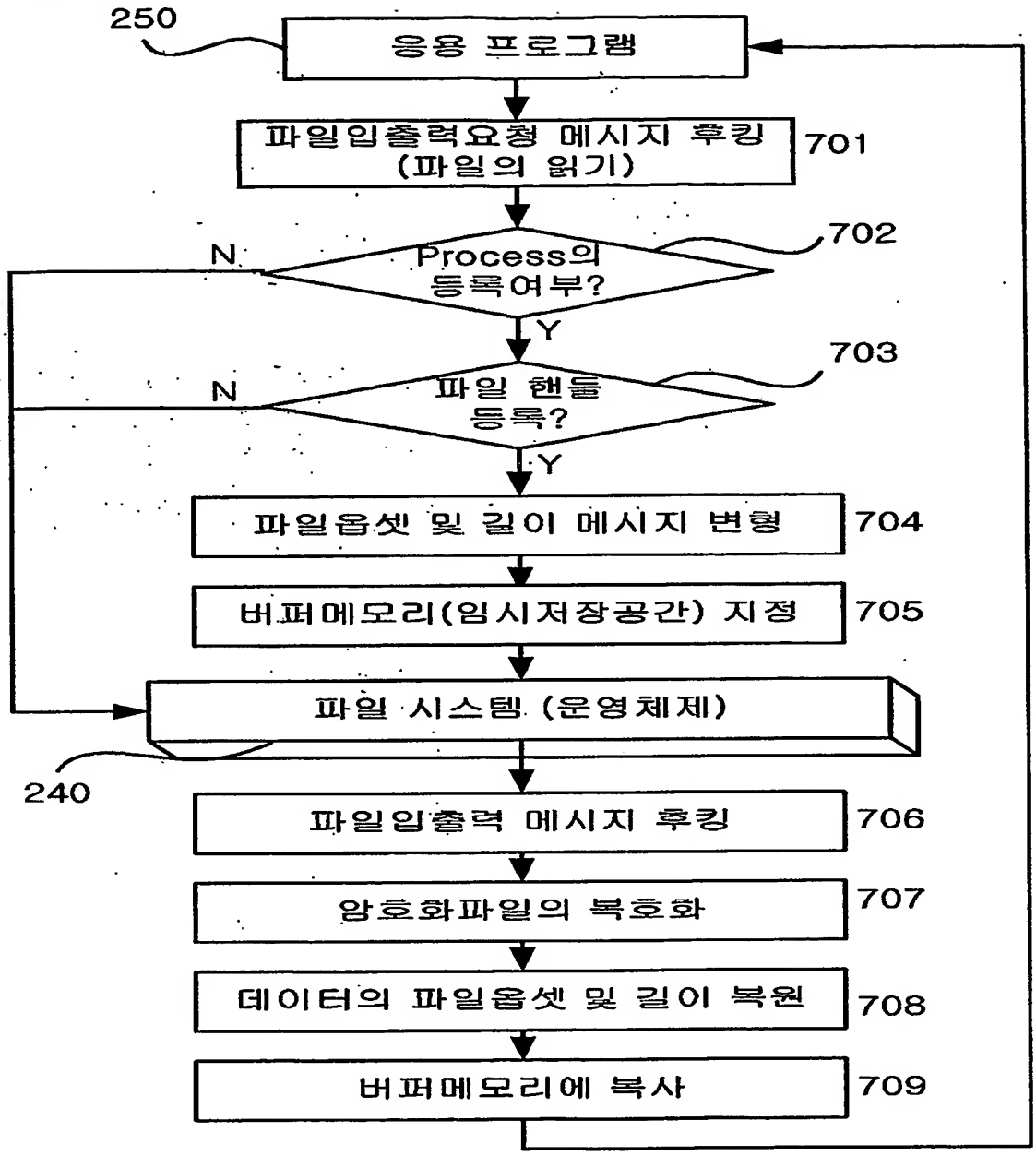
【도 5】


500
사용자
S51
230
210
250
DRM 인증서버
S53
DRM 제어기 (S52)
S54
응용프로그램
S56
S61
사용자레벨
시스템 레벨
220
DRM 디바이스 드라이버
(S57, S60)
S55
S58
S59
240
파일시스템
(암호화된 컨텐츠 패키지)

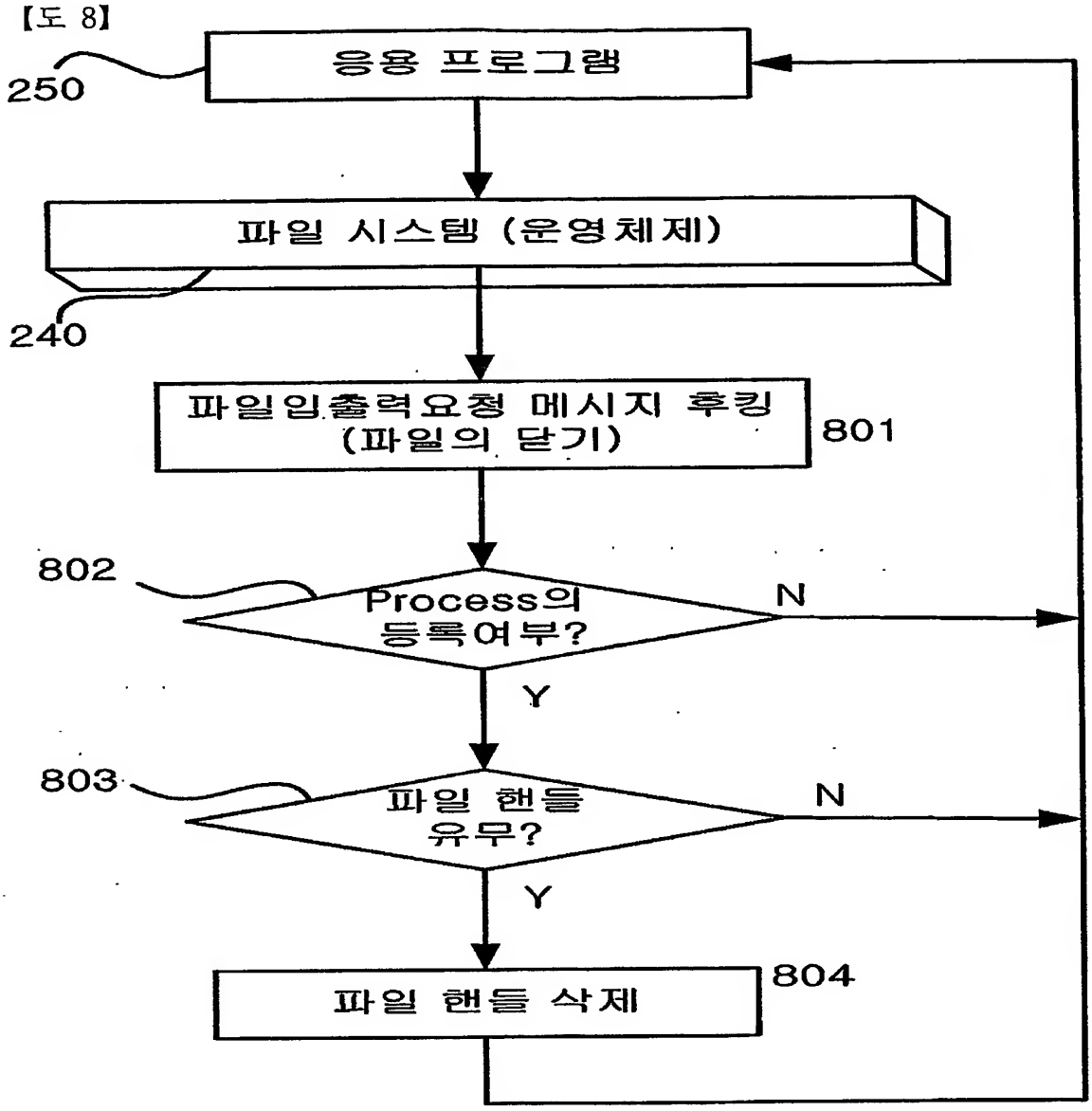
【도 6】


250
응용 프로그램
파일 시스템 (운영체제)
240
601
파일입출력요청 메시지 후킹
(파일의 열기)
602
Process의
등록여부?
N
Y
603
파일이름?
N
Y
604
파일 핸들 등록

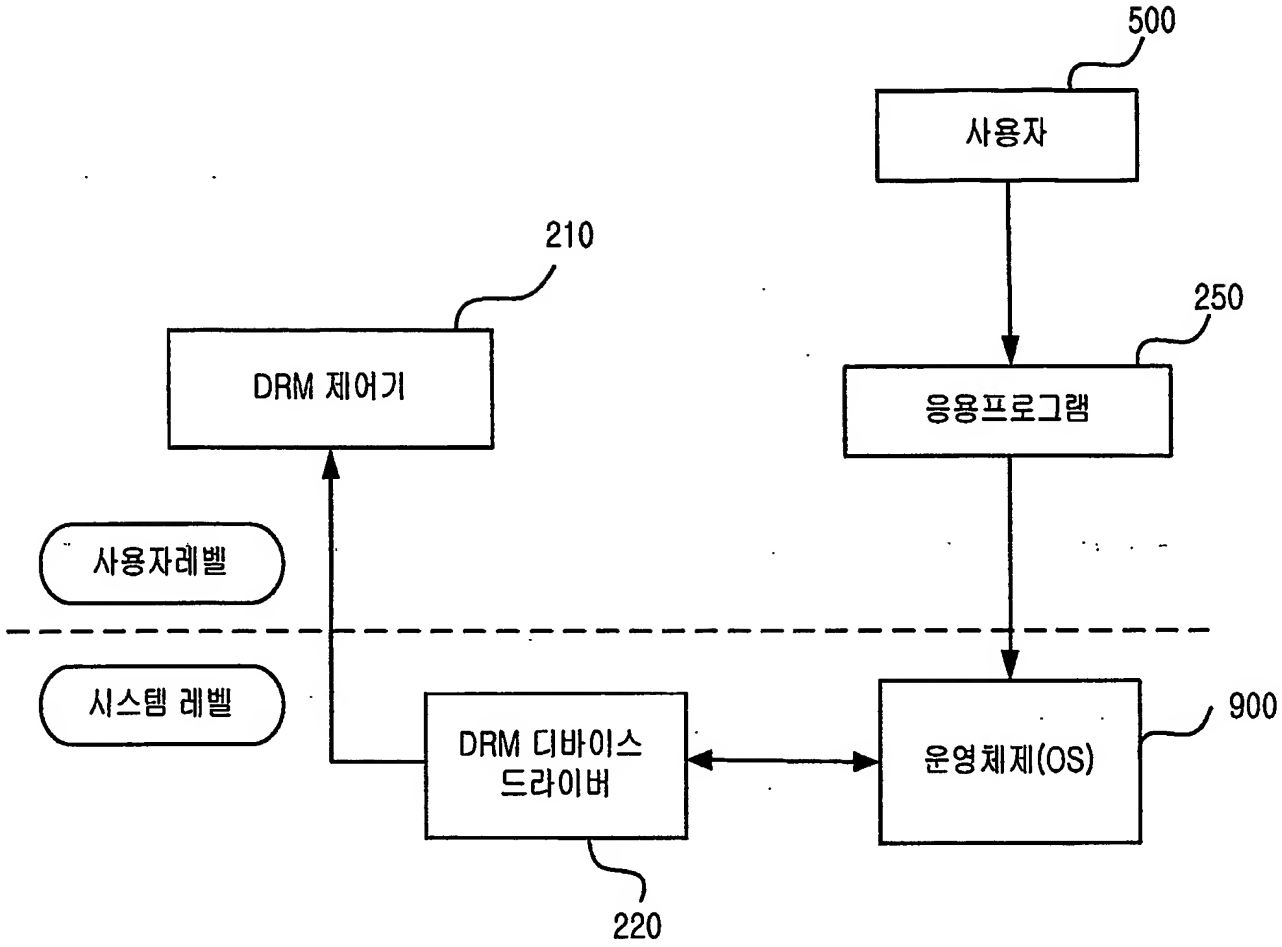
【도 7】


250
응용 프로그램
파일입출력요청 메시지 후킹 (파일의 읽기)
701
Process의 등록여부?
702
N
Y
파일 핸들 등록?
703
N
Y
파일옵셋 및 길이 메시지 변형
704
버퍼메모리(임시저장공간) 지정
705
파일 시스템 (운영체제)
240
파일입출력 메시지 후킹
706
암호화파일의 복호화
707
데이터의 파일옵셋 및 길이 복원
708
버퍼메모리에 복사
709

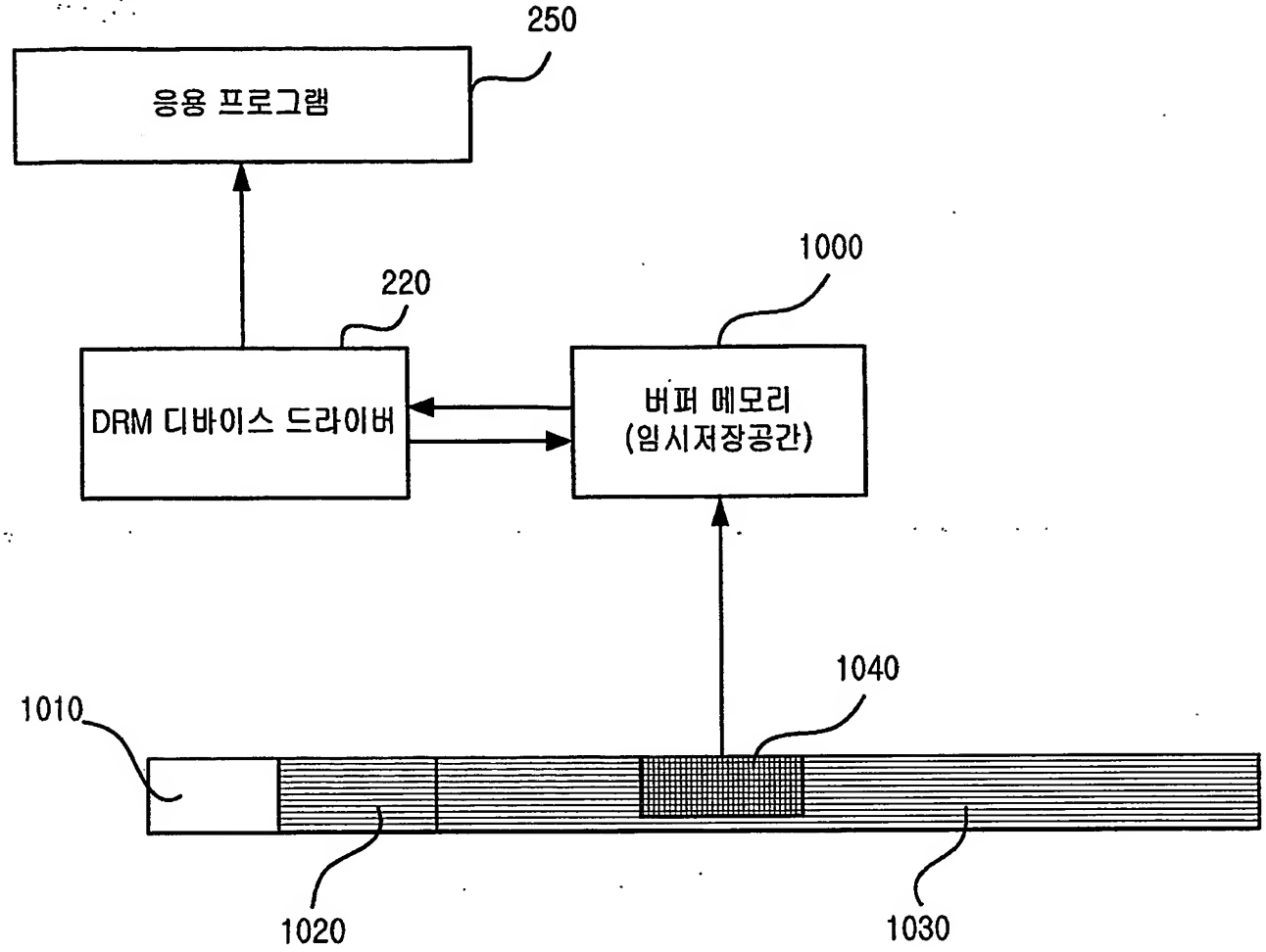
【도 8】


응용 프로그램
250
파일 시스템 (운영체제)
240
파일입출력요청 메시지 후킹
(파일의 닫기)
801
802
Process의
등록여부?
N
Y
803
파일 핸들
유무?
N
Y
804
파일 핸들 삭제

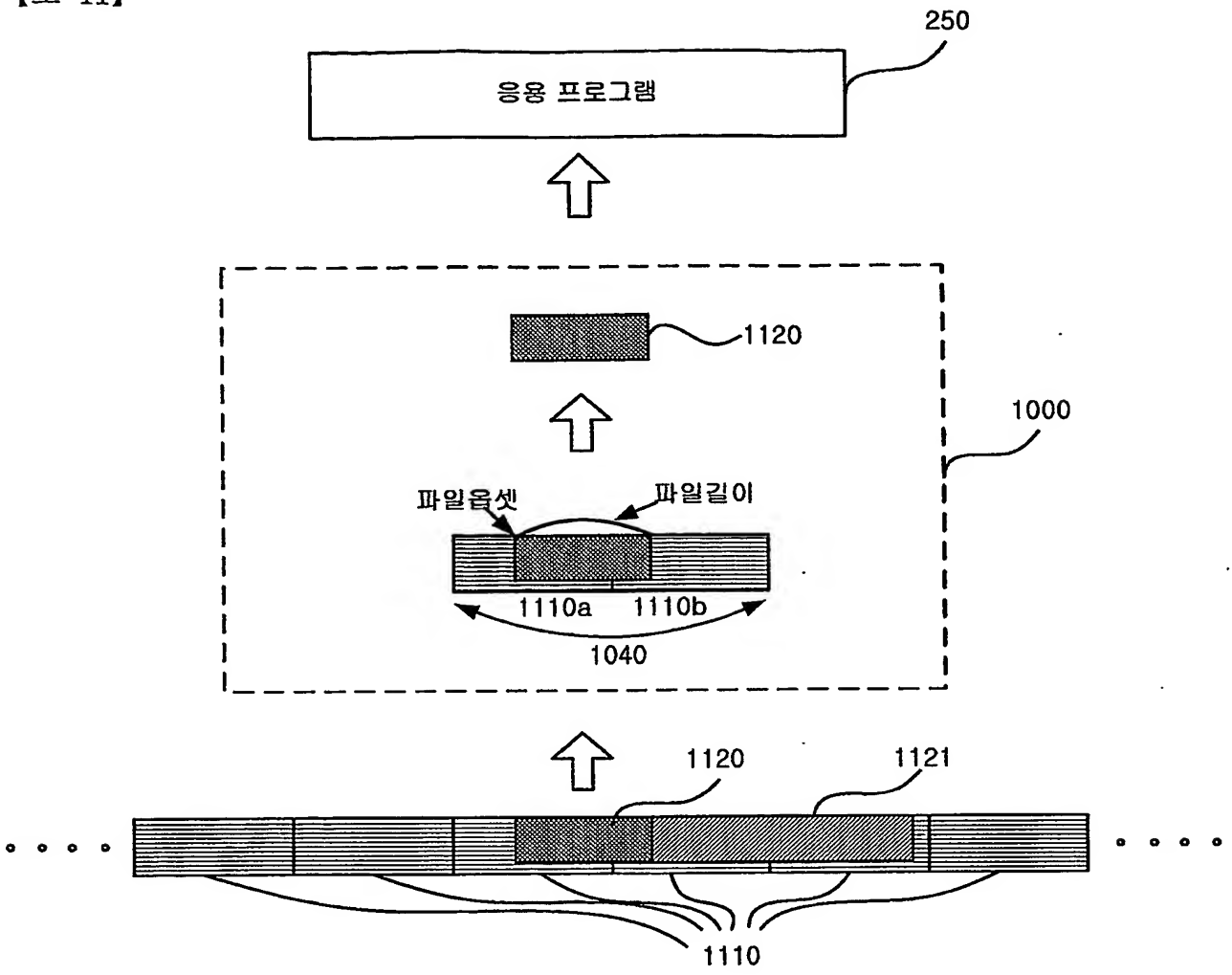
【도 9】


500
사용자
210
DRM 제어기
250
응용프로그램
사용자레벨
시스템 레벨
DRM 디바이스
드라이버
운영체제(OS)
900
220

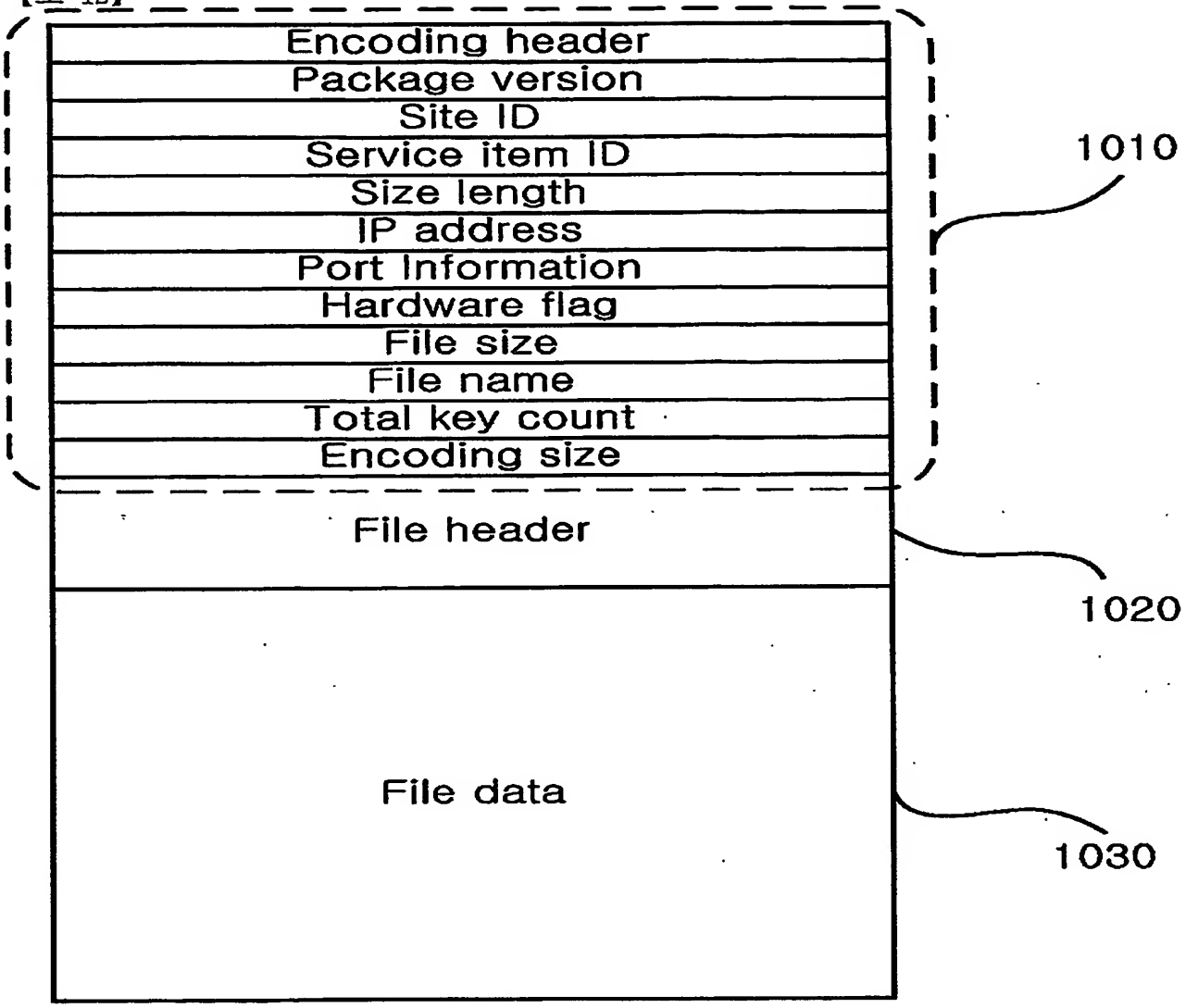
【도 10】


250
응용 프로그램
1000
220
DRM 디바이스 드라이버
버퍼 메모리
(임시저장공간)
1040
1010
1020
1030

【도 11】


250
응용 프로그램
1120
1000
파일옵셋
파일길이
1110a
1110b
1040
1120
1121
1110

【도 12】


Encoding header
Package version
Site ID
Service item ID
Size length
IP address
Port Information
Hardware flag
File size
File name
Total key count
Encoding size
1010
File header
1020
File data
1030

【도 13】

License flag
Start date
End date
Total count
Current count
Total print
Total PC
Current PC
Total Kc index
Current Kc index
Kc
Service item name

【도 14】

【서지사항】

【서류명】	명세서 등 보정서
【수신처】	특허청장
【제출일자】	2003.01.10
【제출인】	
【명칭】	주식회사 코어트러스트
【출원인코드】	1-2000-057231-4
【사건과의 관계】	출원인
【대리인】	
【성명】	홍재일
【대리인코드】	9-1998-000620-8
【포괄위임등록번호】	2002-086159-1
【사건의 표시】	
【출원번호】	10-2002-0001916
【출원일자】	2002.01.12
【심사청구일자】	2002.01.12
【발명의 명칭】	디지털 컨텐츠의 정보보호 방법 및 시스템
【제출원인】	
【접수번호】	1-1-02-0009630-60
【접수일자】	2002.01.12
【보정할 서류】	명세서등
【보정할 사항】	
【보정대상항목】	별지와 같음
【보정방법】	별지와 같음
【보정내용】	별지와 같음
【취지】	특허법시행규칙 제13조·실용신안법시행규칙 제8조의 규정에의하여 위와 같 이 제출합니다. 대리인 홍재일 (인)
【수수료】	
【보정료】	0 원
【추가심사청구료】	0 원
【기타 수수료】	0 원
【합계】	0 원

【보정대상항목】 요약

【보정방법】 정정

【보정내용】

본 발명은 온라인 또는 오프라인으로 제공되는 암호화된 텍스트, 음악, 동영상강의, 영화, 소프트웨어, 게임 등 모든 형태의 디지털 컨텐츠의 불법복제 및 불법전송 등의 저작권 침해행위를 원천적으로 차단하는 정보보호 방법 및 시스템에 관한 것이다.

본 발명의 목적은 암호화된 컨텐츠를 플레이하기 위한 전용뷰어프로그램를 대신에 기존의 일반 응용프로그램을 사용할 수 있고, 다운로드 도중에 스트리밍으로 컨텐츠를 볼 수 있는 한층 보안성능을 높이는 방법 및 시스템과 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는 것이다.

본 발명의 특징은 사용자 컴퓨터의 디바이스 드라이버 단계에서 파일입출력요청 메시지를 후킹하여 메시지의 발생, 변경, 또는 삭제함으로써 일반 응용프로그램을 이용할 수 있는 방법을 제시하는 것이다. 구체적으로는 DRM 디바이스 드라이버 단계에서 응용프로그램이 요청하는 파일옵셋과 파일길이의 메시지를 변경하고, 버퍼메모리상에서 복호화하고, 원래 응용프로그램이 요청한 파일옵셋 및 파일길이 형태의 복호화된 데이터를 복원하여 응용프로그램에 전달하는 방법을 제공하는 것이다.

따라서 본 발명은 디지털 컨텐츠를 복호화된 상태로 어떤 저장장치에 보관하지 않고, 버퍼메모리 상에서만 일정단위로 쪼개진 데이터를 연속적으로 복호화하여 응용프로그램에 전달하기 때문에 암호화가 깨질 염려가 거의 없는 정보보호 방법을 제공하고 있으며, 온라인으로 연결된 DRM 인증서버에서 사용자 인증과 응용프로그램의 등록 및 인증, 관리

를 수행함으로써 사용의 편리성과 업그레이드 관리의 용이성을 크게 향상시키는 효과를 제공한다.

【보정대상항목】 식별번호 19

【보정방법】 정정

【보정내용】

본 발명의 목적은 온라인 또는 오프라인으로 제공되는 디지털 컨텐츠의 정보보호 방법 및 시스템에 관한 것으로서, 좀 더 상세하게는 암호화된 텍스트, 음악, 동영상강의, 영화, 소프트웨어, 게임 등 모든 형태의 디지털 컨텐츠의 불법복제 및 불법전송 등의 저작권 침해행위를 원천적으로 차단하고, 전용뷰어프로그램를 사용하지 않고 기존의 일반 응용프로그램을 사용해서 컨텐츠를 볼 수 있고, 다운로드 중에 스트리밍으로 컨텐츠를 볼 수 있으며, 또한 디바이스 드라이버 단계에서 파일입출력요청 메시지를 후킹(hooking)하여 응용프로그램을 제어함으로서 한층 보안성능을 높인 디지털 컨텐츠의 정보보호 방법 및 시스템과 프로그램 기록매체를 제공하는 것이다.

【보정대상항목】 식별번호 21

【보정방법】 정정

【보정내용】

이러한 디지털 컨텐츠의 불법복제 및 불법배포 문제를 해결하고자 나온 방법 중의 하나가 스트리밍(streaming) 방법이다. 스트리밍 방법은 사용자의 하드디스크에 데이터를 저장하는 것이 아니라 램메모리 상에서만 일시적으로 저장 및 사용이 가능하도록 한 것이지만, 이것은 통신속도 또는 기타 압축 등의 기술적인 문제로 동영상의 끊김, 버퍼링,

엉김 등이 자주 발생하는 단점이 있다. 또한 2001년 7월에 (주)훈넷에서 개발한 하이넷 레코더(Hi Net Recorder)라는 프로그램은 상기 스트리밍 방식으로 서비스되는 인터넷상의 영화, 인터넷방송, 음악, 동영상강의, 뮤직비디오 등을 스트리밍과 동시에 다운로드하여 저장할 수 있음을 보여줌으로써, 스트리밍 방식으로 제공되는 디지털 컨텐츠의 서비스가 불법복제에 취약함을 확인하는 계기가 되었다.

【보정대상항목】 식별번호 22

【보정방법】 정정

【보정내용】

따라서 디지털 컨텐츠의 저작권을 보호하기 위해서 최근 관심이 고조되고 있는 것이 디지털저작권관리(DRM, Digital Rights Management) 시스템이다. DRM 시스템이란 다양한 채널을 통해 유통되는 텍스트, 음악, 이미지, 영상, 동영상강의, 영화, 소프트웨어, 게임 등 각종 디지털 컨텐츠를 불법 복제로부터 보호하고 지속적인 컨텐츠 유료화 서비스를 가능하게 하는 기술이다. 최근 음악파일 무료 다운로드 사이트인 미국의 냅스터에 대한 서비스 중지 판결과 한국판 냅스터인 소리바다에 대한 저작권협회의 소송으로 DRM 시스템에 대한 관심은 어느 때 보다 높아진 상황이며, 이와 같은 저작권 침해 논란을 해결해 줄 수 있는 유일한 대안으로 많은 연구개발 및 상품화가 진행되고 있다. 따라서 컨텐츠 공급자가 DRM 시스템을 도입하면 모든 네트워크를 통해 유통되는 디지털 컨텐츠는 컨텐츠 공급자가 정한 규칙과 사용정책을 충족할 경우에만 열어볼 수 있으며, 불법복제를 하더라도 모든 디지털 컨텐츠는 암호화되어 있어 정당한 비용을 지불하지 않은 사용자는 열어 볼 수가 없게 된다.

【보정대상항목】 식별번호 24

【보정방법】 정정

【보정내용】

DRM 시스템과 관련하여 현재까지 개발된 기술들은 주로 다운로드에 의해 사용자 컴퓨터에 저장되어 있는 암호화된 디지털 컨텐츠에만 적용되거나, 컨텐츠를 보기 위한 전용뷰어프로그램에 DRM 제어기를 내장시킨 방식이 대부분이다. 다운로드 방식에만 적용되는 DRM 시스템의 경우 인터넷영화나 동영상 강의와 같은 대용량의 컨텐츠에 적용하기에는 다운로드 시간이 너무 많이 걸리고, 하드디스크의 용량에 부담이 생기고, 스트리밍을 지원하지 못한다는 단점이 있다. 컨텐츠를 보기 위한 전용뷰어 프로그램에 DRM 제어기가 내장된 경우, 지원되는 컨텐츠 데이터의 파일형식에 제한이 생기고, 수많은 파일형식과 응용프로그램에 대응하는 각각의 전용뷰어프로그램들을 제작해야 하며, 또한 지속적인 전용뷰어프로그램의 업그레이드가 필요한 단점이 있다.

【보정대상항목】 식별번호 25

【보정방법】 정정

【보정내용】

최근 전용뷰어프로그램의 단점을 해소하는 기술로 제안된 것은 '디지털 데이터의 안전한 전달 및 실행을 위한 보안 시스템(한국특허출원 10-2001-0034583, 주식회사 테르텐)'이다. 도 1은 상기 특허출원의 대표도면으로서 일반적인 DRM 프로그램에 적용한 필터단 시스템을 나타내는 모식도이다. 상기 특허의 핵심기술은 클라이언트 시스템의 저장장치에 특정저장영역A(120)를 별도로 생성하고, 특정 실행 프로그램만이 상기 특정저장영역A

에 접근할 수 있도록 필터단을 제어하는 필터단 제어기와, 상기 특정영역내의 모든 데이터의 입출력을 제어하면서 등록된 실행프로그램(B.exe)의 데이터 호출만을 유효한 것으로 판정하여 실행하도록 하는 파일시스템 필터단(130)으로 구성되어 있다. 그러나 상기 기술은 필터단을 통해 응용프로그램을 제어하는 일반적인 기술을 포괄적으로 기술한 것이며, 저장장치 내에 별도관리를 하는 특정저장영역A를 부가적으로 설치가 필요하며, 특정저장영역A에는 복호화된 데이터를 보관함으로써 보안상의 허점이 발생할 수 있으며, 응용프로그램의 등록을 파일시스템 필터단에 모두 등록 및 관리하여야 하며, 암호화 및 복호화에 대한 구체적인 기술적인 언급이 거의 되어있지 않다.

【보정대상항목】 식별번호 28

【보정방법】 정정

【보정내용】

본 발명의 또 다른 목적은 온라인으로 연결된 DRM 인증서버에서 사용자 인증과 응용프로그램의 등록 및 인증, 관리를 수행함으로써 사용의 편리성과 업그레이드 관리의 용이성을 크게 향상시키는 것이다.

【보정대상항목】 식별번호 29

【보정방법】 정정

【보정내용】

본 발명의 또 다른 목적은 디바이스 드라이버 단계에서 파일입출력요청 메시지를 후킹하여 메시지의 발생, 변경, 또는 삭제를 함으로서 응용프로그램을 제어하기 때문에, 암

호화된 컨텐츠를 보기위한 전용뷰어프로그램 대신에 기존의 일반 응용프로그램을 이용할 수 있는 방법을 제안하는 것이다.

【보정대상항목】 식별번호 30

【보정방법】 정정

【보정내용】

본 발명의 또 다른 목적은 DRM 디바이스 드라이버 단계에서 응용프로그램이 요청하는 파일옵셋과 파일길이의 메시지를 변경하고, 복호화하고, 원래 응용프로그램이 요청한 파일옵셋 및 파일길이 형태의 복호화된 데이터를 응용프로그램에 전달하는 방법을 제공하는 것이다.

【보정대상항목】 식별번호 32

【보정방법】 정정

【보정내용】

상기와 같은 목적을 달성하기 위한 본 발명의 디지털 컨텐츠의 정보보호 시스템은, 온라인 또는 오프라인으로 컨텐츠 배포자 서버(260)로부터 제공받아 사용자 컴퓨터에 저장된 암호화된 컨텐츠 패키지를 선택하여 열면 자동으로 DRM 제어기(210)가 구동하여 컨텐츠 패키지 헤더(1010) 속에 포함된 파일이름 및 파일크기, 서버정보, 컨텐츠 정보 등을 수집하여 분석하는 정보분석수단과, 상기 패키지 헤더의 정보분석을 바탕으로 DRM 제어기가 인터넷으로 연결된 DRM 인증서버(230)로 부터 응용프로그램 인증 및 사용자 인증을 수행하는 인증수단과, 상기 인증결과를 바탕으로 DRM 제어기가 획득한 라이센스 파일을 이용하여 컨텐츠의 사용기간 또는 사용횟수, 사용가능한 컴퓨터의 숫자 등의 관리를 하

는 라이센스 관리수단과, 상기 암호화된 컨텐츠 패키지를 볼 수 있는 응용프로그램의 기동 및 제어, 종료 등을 수행하는 제어수단과, DRM 디바이스 드라이버(220)가 응용프로그램과 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템간의 열기, 읽기, 닫기, 종료 등의 파일입출력요청 메시지를 가로채는 디바이스 드라이버 단계의 후킹 수단과, 상기 디바이스 드라이버 단계의 후킹 정보인 응용프로그램이 파일시스템에 요청한 파일옵셋 및 파일길이의 메시지 변경수단과, 상기 변경된 파일옵셋 및 파일길이의 정보를 바탕으로 암호화된 컨텐츠 패키지의 데이터를 버퍼메모리로 가져와서 복호화하는 복호화 수단과, 상기 버퍼메모리에서 복호화된 컨텐츠 패키지의 데이터를 응용프로그램이 요청했던 파일옵셋 및 파일길이 형태로 복원하는 복원수단과, 상기 복호화되어 복원된 컨텐츠 패키지의 데이터를 응용프로그램에 전달하는 전달수단을 포함하는 것을 특징으로 한다.

【보정대상항목】 식별번호 33

【보정방법】 정정

【보정내용】

또한, 상기 목적을 달성하기 위한 본 발명의 디지털 컨텐츠의 정보보호 방법은, 온라인 또는 오프라인으로 컨텐츠 배포자 서버(260)로부터 제공받아 사용자 컴퓨터에 저장된 암호화된 컨텐츠 패키지를 사용자가 선택하여 열면 자동으로 DRM 제어기(210)가 구동하는 단계(S51); 상기 DRM 제어기가 컨텐츠 패키지의 헤더(1010) 속에 포함된 파일이름 및 파일크기, 서버정보, 컨텐츠 정보 등을 수집하여 분석하는 단계(S52); 상기 패키지 헤더의 정보분석을 바탕으로 DRM 제어기가 인터넷으로 연결된 DRM 인증서버(230)로부터 응용프로그램 인증 및 사용자 인증을 수행하여 라이센스 파일의 정보를 획득하는 단계(S53); DRM 제어기가 응용프로그램에게 프로세스 식별자를 생성한 후 응용프로그램의 실

행을 잠시 중지하는 단계(S54); DRM 제어기가 DRM 인증서버로부터 획득한 라이센스 및 응용프로그램 인증정보를 DRM 디바이스 드라이버에 등록시키는 단계(S55); 상기 잠시 중지된 응용프로그램이 다시 구동하여 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템에 파일옵셋과 파일길이를 요청하는 파일입출력요청 메시지를 DRM 디바이스 드라이버에서 후킹하는 단계(S56); 상기 후킹된 파일입출력요청 메시지의 파일옵셋과 파일길이를 암호화된 컨텐츠 패키지의 형태에 맞추어 변경해주는 단계(S57); 상기 변경된 파일옵셋과 파일길이에 맞게끔 암호화된 컨텐츠 패키지의 데이터를 임시저장공간인 버퍼메모리에 로딩하여 복호화하고 원래 응용프로그램이 요청한 파일옵셋과 파일길이에 맞게끔 복호화된 컨텐츠 패키지의 데이터를 복원하는 단계(S60); 및 상기 복원된 파일옵셋과 파일길이에 맞게끔 복호화된 컨텐츠 패키지의 데이터를 응용프로그램에 전송하는 단계(S61)를 포함하는 것을 특징으로 한다.

【보정대상항목】 식별번호 34

【보정방법】 정정

【보정내용】

또한, 상기 목적을 달성하기 위한 본 발명의 기록매체는, 디지털 컨텐츠의 정보보호 시스템에, 온라인 또는 오프라인으로 컨텐츠 배포자로부터 제공받아 사용자 컴퓨터에 저장된 암호화된 컨텐츠 패키지를 사용자가 선택하여 열면 자동으로 DRM 클라이언트 프로그램(200)이 구동하여 컨텐츠 패키지의 헤더 정보를 분석하는 기능; 상기 정보분석을 바탕으로 DRM 클라이언트 프로그램이 인터넷으로 연결된 DRM 인증서버로 부터 응용프로그램 및 사용자 인증을 수행하는 기능; 상기 인증결과를 바탕으로 라이센스를 획득하여 라이센스를 관리하는 기능; 상기 DRM 클라이언트 프로그램이 상기 컨텐츠 패키지를 볼 수 있

는 응용프로그램의 기동 및 제어, 종료 등을 제어하는 기능; 상기 응용프로그램과 파일 시스템간의 파일입출력요청 메시지를 디바이스 드라이버 단계에서 가로채는 후킹기능; 상기 후킹 정보의 파일옵셋 및 파일길이를 변경하는 정보변경 기능; 상기 변경된 파일옵셋 및 파일길이를 바탕으로 암호화된 컨텐츠 패키지의 데이터를 버퍼메모리로 가져와서 복호화하는 기능; 상기 버퍼메모리에서 복호화된 컨텐츠 패키지의 데이터를 응용프로그램이 요청했던 파일옵셋 및 파일길이 형태로 복원하는 기능; 및 상기 복호화되어 복원된 컨텐츠 패키지의 데이터를 응용프로그램에 전달하는 전달기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

【보정대상항목】 식별번호 37

【보정방법】 정정

【보정내용】

도 2는 본 발명의 디지털 컨텐츠의 정보보호 시스템을 나타내는 모식도이다. 먼저 사용자가 인터넷 웹브라우저(280)을 통해 컨텐츠 배포자 서버(260)의 홈페이지에서 사용자 인증(로그인)을 한 후, DRM 제어기(210)와 DRM 디바이스 드라이버(220)로 구성된 DRM 클라이언트 프로그램(200)을 엑티브엑스컨트롤(Active X control)을 이용해 자동으로 다운로드 받아서 신규 또는 업그레이드 설치(S25)한다. 사용자인증이 끝나면 사용자가 선택한 디지털 컨텐츠를 컨텐츠 배포자 서버(260)의 웹서버 혹은 FTP 서버로부터 사용자의 컴퓨터로 다운로드(S26)를 받아서 암호화된 디지털 컨텐츠 패키지를 파일시스템(240)에 저장하게 된다. 상기 암호화된 디지털 컨텐츠 패키지는 일반적으로 컨텐츠 패키저(Contents Packager)라는 프로그램으로 원본 컨텐츠를 암호화하여 컨텐츠 배포자 서버(260)에 업로드시킨 것을 사용자가 다운로드한 것을 의미한다. 여기서 파일시스템이란

파일에 이름을 붙이고, 저장이나 검색을 위해 논리적으로 그것들이 어디에 위치시켜야 하는지 등을 나타내는 것이며, 이와 관련한 운영체제를 일부 포함하는 개념이다. FTP 서버를 이용할 때에는 다운로드만 가능하지만, 웹서버에서 다운로드를 할 때는 HTTP 프로토콜을 이용하여 다운로드와 동시에 다운로드된 컨텐츠 패키지의 용량 안에서 HTTP 스트리밍도 가능하게 된다.

【보정대상항목】 식별번호 38

【보정방법】 정정

【보정내용】

DRM 제어기(210)는 사용자 컴퓨터에 저장되어 있는 암호화된 컨텐츠를 사용하려고 할 때 인터넷으로 연결된 DRM 인증서버(230)로 부터 사용자 인증 및 응용프로그램 인증을 수행하며 이에 대한 내용은 도 3에서 자세히 설명할 것이다. 상술한 바와 같이 컨텐츠 배포자의 홈페이지에 접속해서 컨텐츠를 이용하려고 할 때에는 사용자 로그인 정보를 암호화하여 온라인으로 DRM 인증서버로부터 사용자 인증을 거침으로써 사용자가 중복해서 인증을 받지 않도록 구현한다. DRM 제어기(210)는 컨텐츠 패키지 헤더의 분석 및 라이센스 관리, 응용프로그램의 기동, 제어, 종료 등의 제어기능, 그리고 DRM 디바이스 드라이버(220)의 제어를 수행한다. 컨텐츠의 라이센스 관리는 사용기간 또는 사용횟수, 사용가능한 컴퓨터 숫자 등 컨텐츠 배포자의 필요에 따라 여러 가지로 다양한 조합을 만들 수 있음은 당업자라면 손쉽게 생각할 수 있을 것이다. DRM 디바이스 드라이버(220)는 응용프로그램(250)과 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템(240) 사이에 위치하면서 파일의 열기(open), 읽기(read), 닫기(close) 등을 수행할 때의 파일입출력요청 메시지(File IOREQ, File Input/Output Request Message)를 후킹하여, 상기 메시지와 관

련된 새로운 메시지의 발생, 변경 또는 삭제를 수행함으로써 전용 뷰어프로그램의 개발 없이 기존의 일반 응용프로그램을 이용하여 암호화된 컨텐츠를 볼 수 있도록 제어하며 이에 관해서는 도 6 내지 도 8 부분에서 자세히 설명할 것이다. 또한 DRM 디바이스 드라이버는 응용프로그램이 파일의 읽기를 수행할 때 파일시스템에 요청하는 파일옵셋(file offset) 및 파일길이(file length)에 관련된 파일입출력요청 메시지를 후킹하여 변경하고, 변경된 메시지에 의해 버퍼메모리에 로딩된 암호화된 컨텐츠 패키지의 데이터를 라이센스 파일에 포함된 암호화키를 이용해 복호화하고, 상기 복호화된 데이터를 다시 원래 응용프로그램이 요청했던 파일옵셋과 파일길이 형태의 복원처리하여 응용프로그램에 전달하는 기능을 수행한다. 상기의 파일입출력요청 메시지의 변경 및 복호화, 복원된 데이터의 전달 등 일련의 과정은 실시간으로 데이터의 완전 복호화가 끝날 때까지 연속적으로 진행된다. 또한 DRM 디바이스 드라이버는 응용 프로그램의 종료(Process kill) 메시지를 탐지하고 있다가 상기 메시지를 탐지하면 DRM 제어기에 통보하고 후킹 동작을 멈추게 되며 이에 관해서는 도 9에서 자세히 설명할 것이다. DRM 인증서버(230)는 사용자 인증 및 응용프로그램 인증을 수행하고, 인증에 성공하면 암호화키를 포함한 라이센스 파일을 사용자 컴퓨터의 DRM 제어기에 전달하는 기능을 수행한다. 상기 DRM 인증서버에서의 인증과정은 사용자 컴퓨터와 연계하여 직접 수행하거나, 상술한 바와 같이 인증서버와 인터넷으로 연결된 컨텐츠 배포자 서버(260)와 연계하여 사용자 로그인 정보를 이용하여 자동으로 수행할 수도 있다.

【보정대상항목】 식별번호 39

【보정방법】 정정

【보정내용】

도 3은 본 발명의 DRM 제어기(210)와 DRM 인증서버(230)간의 응용프로그램 인증 및 사용자 인증 방법의 모식도이다. 상술한 바와 같이 DRM 인증서버에서 응용프로그램의 인증을 수행하면 컨텐츠 배포자가 각종 디지털 컨텐츠의 암호화 및 응용프로그램의 업그레이드와 관리적 측면에서 매우 유용한 장점을 가지게 된다. 또한 양방향 세션인증을 이용하여 사용자인증을 수행하면 인터넷상에 패스워드의 이동이 없으므로 보안성능이 높아진다. 먼저 DRM 인증서버(230)의 관리자가 디지털 컨텐츠를 볼 수 있는 응용프로그램의 인증키와 파일용량을 등록시켜 놓는다. 도 4는 DRM 인증서버의 응용프로그램 등록 및 관리 현황을 보여주는 화면의 예시도이다. 그림에서 보듯이 윈도미디어플레이어(Window media player), http 스트리밍 뷰어, GVA, Acrobat reader 등의 디지털 컨텐츠를 볼 수 있는 기존의 일반 응용프로그램을 등록시켜 놓을 수 있다. 따라서 본 발명을 이용하면 일반 문서(아래아 한글, MS워드, 훈민정음 등) 및 MS 오피스(파워포인트, 엑셀, 엑세스 등), 윈도우 미디어 플레이어, 이미지 뷰어, 동영상 강의, 음악 등의 모든 파일 형식을 지원할 수 있으며, DRM 인증서버에 손쉽게 등록하여 업그레이드 등의 관리를 수행할 수 있다. 이때 대부분의 상기 응용프로그램은 손쉽게 등록할 수 있으나, GVA 같은 동영상 강의를 수행하는 프로그램은 파일크기를 체크하는 기능이 있어 원래 파일과 암호화된 파일의 크기가 패키지의 헤더만큼 차이가 생기므로 DRM 클라이언트 프로그램을 만들 때 고려해 주어야만 한다. 도 4의 인증서버의 관리자가 화면 하단의 'Viewer 등록' 아이콘을 선택하면 응용프로그램들을 자유롭게 등록시킬 수 있으며, 화면에는 번호, 인

증된 프로그램, 인증키, 설명, 파일용량, 기능 등의 정보가 표시된다. 본 발명에서 응용프로그램의 인증키는 응용프로그램의 시작점에서 128바이트 후의 16바이트 정보를 16진수로 변환하여 생성하였으며, 응용프로그램의 파일용량을 크기를 정확히 체크하여 응용프로그램의 인증정보로 사용하였으나 당업자라면 얼마든지 비슷한 유형으로 변형할 수 있을 것이다. 도 3의 사용자 컴퓨터에서 응용프로그램의 인증을 받기 위해서는 DRM 제어기(210)가 DRM 인증서버(230)에서의 인증키 생성방법과 동일한 방법으로 자동으로 응용프로그램의 인증키의 생성 및 파일용량의 체크를 수행하여 DRM 인증서버에 전송(S31)한다. DRM 인증서버는 자신이 보관하고 있는 응용프로그램의 인증키 및 파일용량의 값과 사용자 컴퓨터에서 보내온 것을 각각 비교하여 인증성공 또는 인증실패 메시지를 사용자 컴퓨터로 전송(S32)함으로서 응용프로그램의 인증을 수행하게 된다. 만약 사용자 컴퓨터에 관련 응용프로그램이 없다면 인증실패에 관한 메시지를 띄우고, 인증에 성공하면 다음단계로 사용자 인증을 수행하며 상기의 인증순서는 큰 영향을 주지 않는다는 것은 자명하다. 따라서 본 발명의 가장 큰 장점중의 하나는 DRM이 적용된 암호화된 컨텐츠 패키지를 보기 위한 전용 프로그램을 제작할 필요가 없으며, DRM 인증서버에 등록만 시켜준다면 일반 모든 응용프로그램에 본 발명인 디지털 컨텐츠의 정보보호 시스템을 적용할 수 있다는 것이다.

【보정대상항목】 식별번호 40

【보정방법】 정정

【보정내용】

도 3의 사용자 인증을 위해서는 인터넷상으로 사용자의 아이디와 패스워드가 동시에 전송되는 것을 방지하기 위해 양방향 세션인증을 채택하였다. 양방향 세션인증을 위해서는

사용자가 아이디와 패스워드를 입력하게 되면 DRM 제어기(210)에서 임의의 숫자 Rn1 (Random number 1)를 생성하여 사용자 컴퓨터의 하드웨어 정보와 컨텐츠 요청메시지, 임의의 숫자 Rn1을 사용자의 패스워드를 이용해 암호화하게 된다. DRM 제어기(210)는 상기 암호화된 것과 사용자 아이디와 사이트 정보를 DRM 인증서버(230)로 전송(S33)한다. DRM 인증서버는 사용자 아이디와 사이트 정보를 비교한 후, 임의의 숫자 Rn2를 생성하여 서버정보와 Rn1, Rn2, 요청메시지에 대한 응답메시지 등을 사용자 패스워드를 이용해 암호화하여 DRM 제어기로 전송(S34)하게 된다. DRM 제어기는 전송받은 메시지를 복호화하여 상기 생성한 Rn1과 DRM 인증서버에서 수신한 Rn1이 동일한지를 확인한 후, Rn2와 하드웨어정보, 요청메시지를 사용자의 패스워드를 이용해 암호화하고 이것과 사용자 아이디, 사이트 아이디 및 서비스 아이템 아이디 등의 정보를 DRM 인증서버로 전송(S35)한다. DRM 인증서버는 상기 수신한 정보를 복호화한 후 Rn2가 동일한 지를 비교하고 동일하면 사용자의 하드웨어 정보를 인증서버에 등록하고, 사이트 아이디와 서비스아이템 아이디의 라이센스를 검사하고 난 후 라이센스 파일을 하드웨어 정보로 암호화하고 상기 Rn1와 Rn2를 적당히 조합하여 다시 암호화하여 DRM 제어기로 전송(S36)하게 된다. 상기 과정 중에 에러가 발생하지 않는다면 사용자는 라이센스 파일를 획득하게 되며, 상기 과정 중에 한 과정이라도 에러가 발생하게 되면 사용자 인증에 실패함으로써 이와 관련된 메시지를 사용자에게 알려주게 된다. 상술한 방법은 사용자 컴퓨터가 온라인을 이용하여 인증하는 방법이며, 또 다른 인증방법으로는 오프라인으로 CD 또는 디스켓, 기타 저장장치를 이용해 라이센스 파일(300)을 제공(S37)함으로써 인증을 수행할 수 있음은 자명한 사실이다.

【보정대상항목】 식별번호 41

【보정방법】 정정

【보정내용】

도 5는 본 발명의 DRM 시스템의 구성 및 작동을 나타내는 모식도이다. DRM 인증서버(230)는 인터넷으로 사용자 컴퓨터와 연결되어 있으며, 사용자 컴퓨터에서는 사용자레벨에서 작동하는 것은 DRM 제어기(S52)와 응용프로그램(250)이 있으며, 시스템레벨에서 작동하는 것은 DRM 디바이스 드라이버(220)와 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템(240)이다. 암호화된 컨텐츠 패키지가 각각의 DRM 시스템 구성요소와 연계되어 작동하는 것을 살펴보면 다음과 같다. 먼저 사용자(500)가 암호화된 컨텐츠 패키지의 지정된 확장자(.cem) 파일을 열게 되면(S51), 자동으로 연결된 프로그램인 DRM 제어기(210)가 구동된다. DRM 제어기(210)는 암호화된 컨텐츠 패키지의 헤더 정보를 분석(S52)하여 파일이름 및 파일크기, 서버정보, 컨텐츠 정보 등을 수집하여 분석하게 된다. 그 후 DRM 제어기(210)는 DRM 인증서버(230)와 연계하여 상술한 바와 같은 응용프로그램 인증 및 사용자 인증을 수행하여 라이센스 파일을 획득(S53)하게 된다. DRM 제어기가 분석한 컨텐츠 패키지의 헤더 정보에 의해 암호화된 파일이름을 알 수 있으며, DRM 제어기는 파일이름의 확장자를 이용해 관련 응용프로그램(250)을 구동시킨다. 이에 따라 운영체제는 응용프로그램의 구동에 따른 프로세스 식별자(Process Identification Information)를 생성하면, DRM 제어기는 상기 식별자를 획득한 후 응용프로그램의 실행을 잠시 중지(S54)시킨다. DRM 제어기(210)는 라이센스 파일의 암호화키와 프로세스 식별자, 파일이름 등을 DRM 디바이스 드라이버(220)에 등록(S55)을 시켜둔다. 추가적으로 DRM 드라이버에는 나중에 설명할 파일열기가 수행될 때 파일핸들이 등록된다. 상기 각종

데이터의 등록과정 후 응용프로그램(250)이 다시 구동되어 파일 열기 및 읽기, 닫기 명령 등을 수행할 때, DRM 디바이스 드라이버는 상기 파일입출력요청 메시지를 후킹하여 메시지의 발생, 변경, 삭제 등을 수행하며 이것은 도 6, 7, 8에서 자세히 설명할 것이다. 도 5에서는 읽기 과정을 수행할 때 필요한 과정을 자세히 설명할 것이다. 읽기 과정에서는 응용프로그램이 파일시스템에 파일옵셋과 파일길이를 요청(S56)하며, 이것은 각 응용프로그램마다 고유한 값을 가지게 된다. DRM 디바이스 드라이버(220)는 상기 응용프로그램이 요청한 파일옵셋과 파일길이를 후킹한 후, 암호화된 컨텐츠 패키지 형태에 맞추어 16바이트 단위로 파일옵셋과 파일길이의 메시지를 변경처리(S57)해주는 작업을 수행하고 복호화작업을 수행할 버퍼메모리의 주소를 지정한다. 상기 변경된 파일옵셋과 파일길이에 맞게끔 파일시스템(240)에 파일데이터를 요청하고, 요청된 패키지의 데이터를 도 10에서 자세히 설명할 임시저장공간인 버퍼메모리에 로딩하게 된다. 상기 버퍼메모리에서 DRM 디바이스 드라이버는 암호화된 데이터를 라이센스 파일에 포함된 암호화키(Kc)를 이용해 복호화를 수행한 후, 원래 응용프로그램이 요청한 복호화된 파일옵셋과 파일길이의 데이터로 복원처리(S60)를 하여 응용프로그램에 전달(S61)해 준다. 상술한 바와 같이 DRM 디바이스 드라이버(220)가 응용프로그램과 파일시스템 사이의 파일 입출력 메시지를 후킹하고, 메시지를 변경하고, 복호화하고, 복원하는 일련의 필터링 작업을 수행한다. (이하 '필터링'이라함)

【보정대상항목】 식별번호 42

【보정방법】 정정

【보정내용】

본 발명에서의 원본 컨텐츠의 암호화는 Rijndael 알고리즘을 이용하여 16바이트(128비트) 블록 단위로 수행되었다. Rijndael 알고리즘은 벨기에의 암호학자인 Vincent Rijndael 교수가 Joan Daemen과 함께 만들어 낸 것으로, 암호화 알고리즘의 보안성 및 성능, 효율성, 적용성 등의 조화가 타 알고리즘에 비해 탁월한 장점이 있다. 본 발명에서는 Rijndael 알고리즘을 이용해 16바이트(128비트)로 암호화하였으나, 당연히 다른 알고리즘을 이용하거나 32바이트(256비트)등 다른 단위로 암호화시킬 수 있음은 자명한 일이다. 도 5에서 파일옵셋 및 파일길이의 메시지 변경과 데이터 복원이 필요한 이유는, 16바이트 단위로 암호화가 되었기 때문에 정확한 복호화를 위해서는 파일시스템에 16바이트 단위로 파일옵셋 및 파일길이의 데이터를 요청하여 복호화해 주어야 하기 때문이다. 각각의 응용프로그램마다 요청하는 파일옵셋과 파일길이가 모두 틀리기 때문에, DRM 디바이스 드라이버는 응용프로그램과 파일시스템의 중간에 위치하여 파일입출력 요청 메시지를 실시간으로 후킹하여 응용프로램이 요청하는 파일옵셋 및 파일길이 형태로 암호화된 데이터를 복호화하고 다시 복원처리를 해 주어야만 한다. 복호화 및 복원처리는 모두 시스템 레벨에서 작업이 수행되기 때문에 사용자 레벨에서의 응용프로그램은 실제로 DRM 디바이스 드라이버로부터 제공받는 파일데이터가 일반 데이터인지 DRM이 적용된 암호화된 데이터인지를 구분하지 못하게 된다. 또한 응용프로그램과 DRM 디바이스 드라이버 사이에서는 암호가 풀린 상태에서 데이터가 전송되므로, 만약 다른 드라이버가 DRM 드라이버보다 상단에 로딩이 된다면 보안상의 취약점이 발생한다. 따라서 완벽한

보안을 위해서 DRM 디바이스 드라이버는 운영체제에서 필요로 하는 각종 드라이버중의 최상위 레이어에 로딩되어야 한다. 이를 위해 DRM 디바이스 드라이버는 다른 디바이스 드라이버의 로딩을 감시하고 있다가 DRM 디바이스 드라이버위에 다른 디바이스 드라이버가 로딩되는 것을 감지하면 DRM 디바이스 드라이버는 동작을 멈추는 기능을 가지고 있다. 또한 도 9에서 설명이 될 DRM 디바이스 드라이버의 또 다른 기능중의 하나는 응용프로그램의 프로세스 종료 탐지(Process kill detect) 기능이 있다. 이것은 DRM 드라이버가 응용프로그램의 프로세스가 종료되는 것을 감시하고 있다가 종료 메시지를 탐지하면, 종료되는 응용프로그램의 프로세스 식별자와 관련한 모든 자료(파일이름; 암호화키 등)를 모두 삭제하고 DRM 제어기에 통보하게 되고 등록된 프로세스 식별자가 더 이상 없다면 DRM 디바이스 드라이버의 후킹 동작도 멈춤으로써 보안성능을 크게 향상 시킬 수 있게 된다.

【보정대상항목】 식별번호 45

【보정방법】 정정

【보정내용】

도 7은 암호화된 디지털 컨텐츠의 읽기 과정을 보여주는 흐름도이다. DRM 디바이스 드라이버는 응용프로그램이 읽기 명령을 내리면 파일입출력요청 메시지를 후킹(701)하여 응용프로그램의 프로세스 식별자 등록여부를 확인(702)한다. 식별자가 등록되어 있지 않다면 일반 데이터 파일이므로 파일시스템(240)으로 명령을 전달하고, 만약 식별자가 등록되어 있다면 파일핸들의 등록여부를 확인(703)하게 된다. 마찬가지로 파일핸들이 등록되어 있지 않으면 파일시스템으로 명령을 넘기고, 만약 파일핸들이 등록되어 있다면 응용프로그램에서 요구하는 파일옵셋 및 파일길이의 형식을 암호화된 패키지 데이터에 맞

게끔 상기 메시지의 변경처리(704)를 해 준다. 그 후 복호화 작업과 복원작업을 위해 임시저장공간인 버퍼메모리를 지정(705)해주고 파일시스템(240)으로 명령을 전달한다. 파일시스템에서 만들어진 파일입출력요청 메시지를 다시 후킹(706)하여 변경된 파일옵셋 및 파일길이 만큼의 암호화 데이터를 상기 버퍼메모리에 로딩하여 암호화키를 이용해 복호화(707)한다. 그후 복호화된 데이터를 원래 응용프로그램(250)이 요청한 값의 파일옵셋 및 파일길이로 복호화된 데이터를 복원(708)해 주고난 후, 이것을 버퍼메모리에 복사(709)하여 응용프로그램이 읽을 수 있도록 전달해 주게 된다. 상기와 같은 과정을 실시간으로 계속 반복하면서 다른 메시지가 전달될 때까지 암호화된 파일의 복호화를 수행한다. 본 발명에서는 DRM 디바이스 드라이버에서 파일입출력요청 메시지를 후킹하여 파일옵셋 및 파일길이를 변경 및 복원처리를 해 주기 때문에 응용프로그램은 읽기과정을 수행할 때 파일시스템으로부터 전달받는 데이터가 일반 데이터인지 암호화된 것인지 구별하지 못한다. 또한 버퍼메모리에서만 암호화 파일을 16바이트 단위의 조각난 데이터를 복호화하여 응용프로그램에 전달하기 때문에, 사용자가 무단으로 암호화된 파일을 복사하는 것이 원천적으로 봉쇄하게 된다. 결론적으로 DRM 디바이스 드라이버는 읽기 명령일 때 파일입출력요청 메시지의 후킹(701,706)은 파일시스템의 전반부와 후반부에서 모두 수행되며, 주요기능은 파일옵셋 및 파일길이의 메시지 변경 및 암호화파일의 복호화, 복호화된 데이터의 복원작업이다. 또한 DRM 디바이스 드라이버에 복호화 수단 뿐만아니라 암호화 수단을 더 포함하면, 암호화된 컨텐츠의 수정 및 편집, 재저장 등의 기능이 구현될 수 있으며, 이것은 본 발명의 기술적 사상을 이용하여 당업자라면 쉽게 구현할 수 있으므로 여기서는 자세한 설명은 생략한다.

【보정대상항목】 식별번호 48

【보정방법】 정정

【보정내용】

본 발명의 기술적 사상을 이용하면 디바이스 드라이버 단계에서의 파일입출력요청 메시지의 후킹을 수행함으로써 응용프로그램의 열기, 읽기, 닫기 뿐만 아니라, 쓰기, 저장, 복사, 인쇄 등의 일반적 기능을 온(On)/오프(Off) 제어를 할 수 있음은 당업자라면 쉽게 추측할 수 있을 것이다. 또한 본 발명의 디바이스 드라이버 단계의 시스템 제어기술을 사용하면 매크로형태 및 첨부파일에 포함되어 유포되는 e-mail 바이러스의 피해를 방지할 수 있도록, 메일관리 프로그램을 디바이스 드라이버 단계에서 제어하여 첨부파일의 수행을 제한하거나 수행이 되었다고 하더라도 내부자료에 접근하지 못하도록 할 수도 있다.

【보정대상항목】 식별번호 50

【보정방법】 정정

【보정내용】

도 10은 암호화된 디지털 컨텐츠의 복호화 과정을 보여주는 모식도이다. 일반적인 디지털 데이터는 파일헤더(1020)와 데이터(1030)로 구분되어 있다. 따라서 디지털 컨텐츠를 암호화할 때는 특정한 암호화키를 이용해서 파일헤더(1020)와 데이터(1030)를 암호화하게 되며, 파일헤더 앞에 암호화되지 않은 디지털 컨텐츠 패키지의 헤더(1010)를 붙이게 된다. 디지털 컨텐츠 패키지의 헤더(1010)는 도 5에서 설명한 것과 같이 사용자가 지정된 확장자(.cem)의 파일을 선택하여 열면, 자동으로 DRM 제어기(210)가 구동하여 패키지

의 헤더를 분석하여 파일이름 및 파일크기, 서버정보, 컨텐츠정보, 패키지 버전 등의 복호화를 위한 정보를 읽어 들이는데 사용하게 된다. 전술한 바와 같이 응용프로그램이 파일시스템에 요청하는 파일옵셋 및 파일길이 메시지를 DRM 디바이스 드라이버에서 후킹 및 메시지 변경하여 파일시스템에 전달하는 과정은 본 그림에서 생략되어 있고, 복호화 및 복호화된 데이터의 복원과정을 도시하고 있다. 변경된 파일옵셋 및 파일길이 메시지에 해당하는 암호화된 데이터(1040)가 이미 지정되어 있는 버퍼메모리(1000)로 전달되고, DRM 디바이스 드라이버(220)는 버퍼메모리에서 암호화키를 이용해 복호화하며 ; 상기 복호화된 데이터를 원래 응용프로그램이 요청한 파일옵셋 및 파일길이 값으로 복원하여 응용프로그램에 전달하게 된다. 본 그림에서는 생략되어 있지만 디지털 컨텐츠 패키지의 암호화를 하나의 암호화키를 이용하는 방법 또는 보안수준을 높이기 위해 여러 개의 암호화키를 이용해서 암호화 및 복호화를 할 수도 있다. 예를 들면 암호화해야할 디지털 컨텐츠의 용량이 50메가바이트이라면, 10메가바이트씩 5개의 암호화키를 이용해서 암호화를 수행하고 관련 정보를 컨텐츠 패키지의 헤더와 라이센스 정보파일에 기록하여 복호화를 수행함으로써 보안수준을 한층 더 높일 수 있다.

【보정대상항목】 식별번호 51

【보정방법】 정정

【보정내용】

도 11은 암호화된 디지털 컨텐츠의 파일옵셋과 파일길이를 처리하는 과정을 보여주는 모식도이다. 본 발명의 실시예에서는 Rijndael 알고리즘을 사용하기 때문에 16바이트 (128비트) 단위로 암호화 및 복호화가 이루어지며, 그림에서 암호화된 데이터 블록

(1110)들은 동일하게 16바이트로 암호화 된 것을 보여준다. 응용프로그램이 요청한 실제 파일옵셋 및 파일길이에 해당하는 데이터블록(1120)이 16바이트 단위의 데이터블록 두개(1110a와 1110b)에 걸쳐 있다면, 상기 암호화된 두개의 데이터블록에 맞게끔 파일옵셋 및 파일길이 메시지를 변경하여서 파일시스템에 전달하게 되며 이 과정은 본 그림에서 생략되어 있다. 따라서 변경된 파일옵셋과 파일길이 메시지에 해당하는 두개의 데이터블록(1110a와 1110b)을 모두 버퍼메모리(1000)에 로딩하여, DRM 디바이스 드라이버에 등록되어 있는 암호화키를 이용하여 복호화하고 난 후 원래 응용프로그램(250)이 요청했던 파일옵셋과 파일길이 형태의 데이터로 복원처리하여 만들어진 데이터블록(1120)을 응용프로그램(250)에 전달하게 된다. 그 후 응용프로그램이 요청하는 다음순서의 파일데이터에 해당하는 임의의 크기인 데이터블록(1121)도 상기와 똑같은 과정을 거친 후 응용프로그램에 전달하는 과정을 거치게 된다. 본 과정은 실시간으로 버퍼메모리상에서 일어나기 때문에 도 2에서 설명한 바와 같이 컨텐츠 배포자 서버(260)의 웹서버 및 FTP 서버로부터 다운로드(S26)하여 저장된 암호화된 컨텐츠 패키지 뿐만 아니라, HTTP 프로토콜을 이용해서 다운로드 과정과 동시에 HTTP 스트리밍 서비스도 가능하게 된다. 이것은 본 발명의 중요한 특징 중의 하나로서 기존의 DRM 시스템이 일반적으로 다운로드가 완료된 암호화된 컨텐츠에 대해서만 적용할 수 있는데 비해서, 본 발명은 다운로드를 완료한 컨텐츠 뿐만 아니라 다운로드 중에 HTTP 스트리밍 서비스도 가능하게 된다. 이것은 온라인 강의나 인터넷영화, 동영상파일등의 대용량의 디지털 컨텐츠에 DRM 시스템을 적용할 경우 다운로드를 받는 시간동안 사용자가 불편하게 기다리던 불편을 완전히 해소한 매우 유리한 장점을 가지게 된다. 또한 본 발명을 통해 웹서버를 통한 HTTP 스트리밍 서비스가 다운로드와 동시에 이루어지므로 컨텐츠 배포자 서버(260)가 DRM을 적용한 디지털 컨텐츠

의 스트리밍 서비스를 위해 필요한 MMS (Microsoft windows Media Server) 서버 등의 구입 및 운영 비용을 절감할 수 있는 장점을 가진다.

【보정대상항목】 식별번호 54

【보정방법】 정정

【보정내용】

도 14는 본 발명의 일실시예에 따른 DRM이 적용된 HTTP 스트리밍을 보여주는 동영상강의 화면의 예시도이다. HTTP 프로토콜을 사용하는 웹서버를 이용하여 디지털 컨텐츠를 다운로드 받을 때, 다운로드와 동시에 HTTP 스트리밍이 이루어지는 것을 보여주고 있다. 동영상 강의 화면의 아래부분에 약간 희게 나타난 경계부분이 실제 다운로드가 진행되는 상태를 보여주는 것이며, 작은 직사각형의 상태바(status bar)는 현재 스트리밍이 진행되는 위치를 보여준다. 사용자는 HTTP 스트리밍만을 이용할 것인지, HTTP 스트리밍 및 다운로드 서비스를 동시에 이용할 것이지, 또한 디지털 컨텐츠의 저장위치와 파일이름을 결정할 수 있다. 따라서 완벽한 디지털 컨텐츠의 정보보호가 이루어진 상태에서 다운로드와 동시에 스트리밍을 진행할 수 있음을 알 수 있다.

【보정대상항목】 식별번호 56

【보정방법】 정정

【보정내용】

본 발명에서 제안한 디지털 컨텐츠의 정보보호 방법 및 시스템은 일반 응용프로그램의 시스템 레벨에서의 디바이스 드라이버 제어기술을 사용함으로써, 전용뷰어프로그램의 개발없이 기존의 다양한 응용프로그램을 사용함으로서 현재 통용되고 있는 모든 컨텐츠 파

일형식에 적용되는 일반적인 DRM 시스템을 구축할 수 있도록 해줌으로써 향후 새로운 종류의 컨텐츠에 능동적으로 대응할 수 있다.

【보정대상항목】 식별번호 59

【보정방법】 정정

【보정내용】

본 발명의 시스템을 이용하면 중요한 문서나 컨텐츠를 보호하기 위해서 임의의 파일에 대한 접근 허용을 시스템 단계에서 제어함으로써, 허가받지 않은 사람들에 대한 접근제어를 할 수 있다. 또한 특정파일을 이용하는 응용프로그램에 대하여 시스템단계에서의 다양한 파일조작을 통한 새로운 서비스를 개발할 수 있다.

【보정대상항목】 식별번호 60

【보정방법】 정정

【보정내용】

또한 디바이스 드라이버 단계에서의 파일입출력요청 메시지의 후킹을 수행함으로써 응용프로그램의 열기, 읽기, 닫기 뿐만 아니라, 쓰기, 저장, 복사, 인쇄 등의 일반적 기능을 온(On)/오프(Off) 제어를 할 수 있다.

【보정대상항목】 청구항 1

【보정방법】 정정

【보정내용】

각각 CPU, 휘발성 저장장치(메모리), 비휘발성 저장장치(하드디스크), 입출력장치(키보드, 모니터 등)를 가지며, 유무선 내부 통신수단이나 외부 네트워크와의 통신수단에 의

하여 연결되어 있는 컨텐츠 배포자 서버(260)와 DRM 인증서버(230), 사용자 컴퓨터로 구성된 디지털 컨텐츠의 정보보호 시스템에 있어서,

상기 컨텐츠 배포자서버(260)는

컨텐츠 패키저 프로그램을 이용하여 원본 콘텐츠를 암호화한 컨텐츠 패키지를 저장하고 사용자의 요청에 따라 암호화된 컨텐츠 패키지를 다운로드 또는 스트리밍 방식으로 전달하는 수단을 구비하며,

상기 DRM 인증서버(230)는

원본 컨텐츠를 암호화하기 위한 암호화키의 생성 및 암호화된 컨텐츠를 사용할 수 있는 각종 사용권한 정보를 가지는 라이센스 파일을 발급하고 관리하는 라이센스 발급관리 수단과,

사용자 컴퓨터와 연결하여 사용자 및 프로그램 등의 각종 인증을 수행하는 인증 수단을 구비하며,

상기 사용자 컴퓨터는

온라인 또는 오프라인으로 컨텐츠 배포자 서버(260)로부터 제공받아 사용자 컴퓨터에 저장된 암호화된 컨텐츠 패키지를 선택하여 열면 자동으로 DRM 제어기(210)가 구동하여 컨텐츠 패키지 헤더(1010) 속에 포함된 파일이름 및 파일크기, 서버정보, 컨텐츠 정보 등을 수집하여 분석하는 정보분석수단과,

상기 패키지 헤더의 정보분석을 바탕으로 DRM 제어기가 인터넷으로 연결된 DRM 인증서버(230)로 부터 응용프로그램 인증 및 사용자 인증을 수행하는 인증수단과,

상기 인증결과를 바탕으로 DRM 제어기가 획득한 라이센스 파일을 이용하여 컨텐츠의 사용기간 또는 사용횟수, 사용가능한 컴퓨터의 숫자 등의 관리를 하는 라이센스 관리수단과,

상기 암호화된 컨텐츠 패키지를 볼 수 있는 응용프로그램의 기동 및 제어, 종료 등을 수행하는 제어수단과,

DRM 디바이스 드라이버(220)가 상기 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템과 기존의 응용프로그램 사이에 위치하면서 메시지의 후킹, 변경, 복호화, 복원하는 필터링 수단을 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【보정대상항목】 청구항 2

【보정방법】 정정

【보정내용】

제 1항에 있어서, 상기 필터링 수단은

DRM 디바이스 드라이버(220)가 응용프로그램과 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템간의 열기, 읽기, 닫기, 종료 등의 파일입출력요청 메시지를 가로채는 디바이스 드라이버 단계의 후킹 수단과,

상기 디바이스 드라이버 단계의 후킹 정보인 응용프로그램이 파일시스템에 요청한 파일옵셋 및 파일길이의 정보변경수단과,

상기 변경된 파일옵셋 및 파일길이의 정보를 바탕으로 암호화된 컨텐츠 패키지의 데이터를 버퍼메모리로 가져와서 복호화하는 복호화 수단과,

상기 버퍼메모리에서 복호화된 컨텐츠 패키지의 데이터를 응용프로그램이 요청했던 파일 옵셋 및 파일길이 형태로 복원하는 복원수단과,

상기 복호화되어 복원된 컨텐츠 패키지의 데이터를 응용프로그램에 전달하는 전달수단을 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【보정대상항목】 청구항 3

【보정방법】 정정

【보정내용】

제 1항에 있어서,

상기 암호화된 컨텐츠 패키지는 원본 컨텐츠를 하나의 암호화키 또는 여러 개의 암호화키를 이용하여 암호화한 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【보정대상항목】 청구항 4

【보정방법】 정정

【보정내용】

제 1항에 있어서,

상기 DRM 디바이스 드라이버(220)가 운영체제에서 필요한 각종 디바이스 드라이버중 최상위 레이어에 로딩될 수 있도록, 다른 디바이스 드라이버가 로딩되는 것을 감지하면 DRM 디바이스 드라이버의 동작을 멈추게 하는 디바이스 드라이버 감시수단을 더 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【보정대상항목】 청구항 5

【보정방법】 정정

【보정내용】

제 1항에 있어서,

상기 암호화된 컨텐츠 패키지는 사용자 컴퓨터의 파일 시스템(240)에 모두 다운로드 받아 저장하고 난 후 컨텐츠를 플레이하는 것 대신에 컨텐츠 배포자 서버(260)로부터 다운로드 받아 저장하는 것과 동시에 실시간으로 복호화하여 HTTP 스트리밍 방식으로 컨텐츠를 플레이할 수 있는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【보정대상항목】 청구항 6

【보정방법】 정정

【보정내용】

제 1항 내지 제 5항 중 어느 한 항에 있어서,

상기 DRM 디바이스 드라이버(220)는 응용프로그램이 읽어들인 복호화된 디지털 컨텐츠의 데이터를 수정 또는 편집하여 다시 저장할 수 있도록 암호화 수단을 더 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 시스템.

【보정대상항목】 청구항 7

【보정방법】 정정

【보정내용】

각각 CPU, 휘발성 저장장치(메모리), 비휘발성 저장장치(하드디스크), 입출력장치(키보드, 모니터 등)를 가지며, 유무선 내부 통신수단이나 외부 네트워크와의 통신수단에 의

하여 연결되어 있는 컨텐츠 배포자 서버(260)와 DRM 인증서버(230), 사용자 컴퓨터로 구성된 디지털 컨텐츠의 정보보호 시스템에 있어서,

상기 DRM 인증서버(230)에서 생성한 하나 또는 여러 개의 암호화키를 이용하여 원본 컨텐츠를 암호화하여 암호화된 컨텐츠 패키지를 제작하고 이를 컨텐츠 배포자 서버(260)에 업로드하는 암호화 및 업로드 단계와;

사용자가 컨텐츠 배포자 서버(260)의 홈페이지에서 원하는 암호화된 컨텐츠 패키지를 선택하여 사용자 컴퓨터에 다운로드 또는 스트리밍으로 저장하는 전달 및 저장 단계와;

암호화된 컨텐츠 패키지를 볼 수 있는 사용권한을 확인하는 라이센스 파일을 분석하여 각종 인증을 수행하는 인증 단계와;

인증 성공 후 DRM 디바이스 드라이버가 암호화된 컨텐츠 패키지를 필터링하고 복호화하여 플레이할 수 있도록 응용프로그램에 전달하는 필터링 및 플레이 단계와;

상기 필터링 및 플레이 단계에서 DRM 디바이스 드라이버가 응용프로그램의 종료메시지를 탐지하면 등록된 프로세스 식별자와 관련한 모든 자료를 삭제하고 DRM 제어기에 종료메시지를 통보하고 드라이버 상에 더 이상 등록된 식별자가 없다면 후킹 동작을 멈추는 종료단계;

로 구성되는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 방법.

【보정대상항목】 청구항 8

【보정방법】 정정

【보정내용】

제 7항에 있어서, 필터링 및 플레이 단계는 온라인 또는 오프라인으로 컨텐츠 배포자 서버(260)로부터 제공받아 사용자 컴퓨터에 저장된 암호화된 컨텐츠 패키지를 사용자가 선택하여 열면 자동으로 DRM 제어기(210)가 구동하는 단계(S51);

상기 DRM 제어기가 컨텐츠 패키지의 헤더(1010) 속에 포함된 파일이름 및 파일크기, 서버정보, 컨텐츠 정보 등을 수집하여 분석하는 단계(S52);

상기 패키지 헤더의 정보분석을 바탕으로 DRM 제어기가 인터넷으로 연결된 DRM 인증서버(230)로부터 응용프로그램 인증 및 사용자 인증을 수행하여 라이센스 파일의 정보를 획득하는 단계(S53);

DRM 제어기가 응용프로그램에게 프로세스 식별자를 생성한 후 응용프로그램의 실행을 잠시 중지하는 단계(S54);

DRM 제어기가 DRM 인증서버로부터 획득한 라이센스 및 응용프로그램 인증정보를 DRM 디바이스 드라이버에 등록시키는 단계(S55);

상기 잠시 중지된 응용프로그램이 다시 구동하여 암호화된 컨텐츠 패키지가 저장되어 있는 파일시스템에 파일옵셋과 파일길이를 요청하는 파일입출력요청 메시지를 DRM 디바이스 드라이버에서 후킹하는 단계(S56);

상기 후킹된 파일입출력요청 메시지의 파일옵셋과 파일길이를 암호화된 컨텐츠 패키지의 형태에 맞추어 변형해주는 단계(S57);

상기 변형된 파일옵셋과 파일길이에 맞게끔 암호화된 컨텐츠 패키지의 데이터를 임시저장공간인 버퍼메모리에 로딩하여 복호화하고 원래 응용프로그램이 요청한 파일옵셋과 파일길이에 맞게끔 복호화된 컨텐츠 패키지의 데이터를 복원하는 단계(S60);

상기 복원된 파일옵셋과 파일길이에 맞게끔 복호화된 컨텐츠 패키지의 데이터를 응용프로그램에 전달하는 단계(S61);

를 더 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 방법.

【보정대상항목】 청구항 9

【보정방법】 정정

【보정내용】

제 7항에 있어서,

상기 DRM 디바이스 드라이버는 운영체제에서 필요한 각종 디바이스 드라이버중 최상위 레이어에 로딩될 수 있도록, 다른 디바이스 드라이버가 로딩되는 것을 감지하면 DRM 디바이스 드라이버의 동작을 멈추는 단계를 더 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 방법.

【보정대상항목】 청구항 10

【보정방법】 정정

【보정내용】

제 7항에 있어서,

상기 암호화된 컨텐츠 패키지는 사용자 컴퓨터의 파일 시스템(240)에 모두 다운로드 받아 저장하고 난 후 컨텐츠를 플레이하는 것 대신에 컨텐츠 배포자 서버(260)로부터 다운

로드 받아 저장하는 것과 동시에 실시간으로 복호화하여 HTTP 스트리밍 방식으로 컨텐츠를 플레이할 수 있는 단계를 더 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 방법.

【보정대상항목】 청구항 11

【보정방법】 정정

【보정내용】

제 7항 내지 제 10항 중 어느 한 항에 있어서,

상기 DRM 디바이스 드라이버는 응용프로그램이 읽어들인 복호화된 디지털 컨텐츠의 데이터를 수정 또는 편집하여 다시 저장할 수 있도록 DRM 디바이스 드라이버에 암호화하는 단계를 더 포함하는 것을 특징으로 하는 디지털 컨텐츠의 정보보호 방법.

【보정대상항목】 청구항 12

【보정방법】 정정

【보정내용】

각각 CPU, 휘발성 저장장치(메모리), 비휘발성 저장장치(하드디스크), 입출력장치(키보드, 모니터 등)를 가지며, 유무선 내부 통신수단이나 외부 네트워크와의 통신수단에 의하여 연결되어 있는 컨텐츠 배포자 서버(260)와 DRM 인증서버(230), 사용자 컴퓨터로 구성된 디지털 컨텐츠의 정보보호 시스템에 있어서,

상기 DRM 인증서버(230)에서 생성한 하나 또는 여러 개의 암호화키를 이용하여 원본 컨텐츠를 암호화하여 암호화된 컨텐츠 패키지를 제작하고 이를 컨텐츠 배포자 서버(260)에 업로드하는 암호화 및 업로드 단계와;

사용자가 컨텐츠 배포자 서버(260)인 웹서버 또는 FTP 서버의 홈페이지에 접속하여 회원가입하고 DRM 클라이언트 프로그램을 다운로드하여 설치하는 회원가입 및 설치 단계와;

사용자가 컨텐츠 배포자 서버(260)의 홈페이지에서 원하는 암호화된 컨텐츠 패키지를 선택하여 사용자 컴퓨터에 다운로드 또는 스트리밍으로 저장하는 전달 및 저장 단계와;

암호화된 컨텐츠 패키지를 볼 수 있는 사용권한을 확인하는 라이센스 파일을 분석하여 각종 인증을 수행하는 인증 단계와;

인증 성공 후 암호화된 컨텐츠 패키지를 복호화하여 플레이할 수 있도록 응용프로그램에 전달하는 복호화 및 플레이 단계와;

상기 필터링 및 플레이 단계에서 DRM 디바이스 드라이버가 응용프로그램의 종료메시지를 탐지하면 등록된 프로세스 식별자와 관련한 모든 자료를 삭제하고 DRM 제어기에 종료메시지를 통보하고 드라이버 상에 더 이상 등록된 식별자가 없다면 후킹 동작을 멈추는 종료단계;

로 구성되는 것을 특징으로 하는 디지털 컨텐츠의 정보보호하는 방법이 저장되어 있는 컴퓨터로 실행할 수 있는 기록매체.

【보정대상항목】 청구항 13

【보정방법】 삭제

【보정대상항목】 청구항 14

【보정방법】 삭제

【보정대상항목】 청구항 15

【보정방법】 삭제